TECHNICKÁ UNIVERZITA V LIBERCI

Fakulta mechatroniky a mezioborových inženýrských studií

Studijní program: B 2612 – Elektrotechnika a informatika

Studijní obor: 2612R011 – Elektronické informační a řídicí systémy

NÁVRH BT MODULU PRO KOMUNIKACI S PDA ZAŘÍZENÍM

DESIGN OF THE BT MODULE FOR COMMUNICATION WITH PDA

BAKALÁŘSKÁ PRÁCE

Autor: **Jan Pleva**

Vedoucí BP práce: Ing. Jaroslav Buchta

V Liberec 15. 5. 2006

Originál zadání práce

Prohlášení:

Byl(a) jsem seznámen(a) s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 o právu autorském, zejména § 60 (školní dílo).

Beru na vědomí, že TUL má právo na uzavření licenční smlouvy o užití mé BP a prohlašuji, že **s o u h l a s í m** s případným užitím mé bakalářské práce (prodej, zapůjčení apod.).

Jsem si vědom(a) toho, že užít své bakalářské práce či poskytnout licenci k jejímu využití mohu jen se souhlasem TUL, která má právo ode mne požadovat přiměřený příspěvek na úhradu nákladů, vynaložených univerzitou na vytvoření díla (až do jejich skutečné výše).

Bakalářskou práci jsem vypracoval(a) samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

Datum

Podpis

Poděkování:

Děkuji za cenné rady, podměty a připomínky vedoucímu bakalářské práce Ing. Jaroslavu Buchtovi.

Neméně díků patří i mým rodičům za neklesající důvěru a podporu. Dále můj velký vděk patří „J“-ovi, Jakubovi Z., Honzovi B., Helče M., Tině S., Johance K., Standovi N. a všem mým kamarádům, kteří mě podporovali i jinak, než jen odbornými radami.

Abstrakt

Cílem bakalářské práce je seznámení s bezdrátovou technologií Bluetooth. Práce pojednává o principech tvorby sítí a popisuje jednotlivé stavy uzlů při komunikaci. Shrnuje technické možnosti Bluetooth. Popisuje vrstvy a jejich role v propracované struktuře Bluetooth jednotky. Práce se též zaobírá bezpečností a hrozbami zneužití párování přístrojů. Jsou doporučena základní pravidla pro bezpečné spojení dvou Bluetooth zařízení.

Rozsah možností využití Bluetooth je velmi pestrý. Technologie nalézá uplatnění jak v domácím prostředí, tak i v pracovních podmínkách. Díky své miniaturizaci a čím dál lepší dostupnosti je velmi často uplatňována v mobilních zařízeních. Výslednou prací je praktický návrh a propojení Bluetooth modulu BlueNiceCom III s mikroprocesorem Atmega8. Řídící mikrokontroler se stará o správné fungování Bluetooth modulu přes rozhraní UART.

Klíčová slova: Bluetooth, bezdrátová technologie, komunikace, BT modul

Abstract

The goal of the Bachelor's work is to provide introduction to the Blootooth wireless technology. The work deals with the principles of network creation and describes conditions of members during communication. It summarizes technical possibilities of Bluetooth and describes layers and their roles in the sophisticated structure of the Bluetooth unit. The work also deals with security and the threat that device pairing presents. Basic rules for secure connection of two Bluetooth devices are recommended.

The usage of Bluetooth is very versatile. The technology can be used both at home and at work. Due to its miniaturization and increasingly better availability it is very often used in mobile devices. The final work is a practical proposal and the connection of BlueNiceCom III Bluetooth module with Atmega 8 microprocessor. The operating microcontroller is responsible of the right function of Bluetooth module through the UART interface.

Keywords: Bluetooth, wireless technology, communication, BT module

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM POUŽITÝCH ZKRATEK

BSIG *Bluetooth Special Interest Group*
pracovní skupina pro vývoj standardu Bluetooth

EDR *Enhanced Data Rate*
metoda pro větší rychlost přenosu dat

AFH *Adaptive Frequency Hopping*
přizpůsobované kmitočtové změny

TDMA *Time Division Multiple Access*
časové dělení mnohonásobného přístupu

FHSS *Frequency Hopping Spread Spectrum*
přeskoková frekvence na rozprostřeném spektru

QoS *Quality of Service*
kvalita poskytované služby

TDD *Time Division Duplexing*
časové rozdělení provozu

WLAN *Wireles LAN*
bezdrátová LAN

WEP *Wired Equivalent Privacy*
šifrovací protokol

BAP *Bluetooth Access Point*
přístupový bod Bluetooth

AMA *Active Member Address*
Adresa pro aktivní uzel

PMA *Parked Member Address*
Adresa pro odstavený uzel

PDA *Pesonal Digital Assistant*
Osobní digitální asistent – kapesní počítač

ISM *Industrial, Scientific, Medicine*
Bezlicenční pásmo pro průmysl, vědu a zdravotnictví

I/O *input / output*
Vstupy / výstupy

BT *Bluetooth*
Bezdrátová technologie

GSM *Global System for Mobile Communications*
Globální mobilní systém

Wi-Fi *Wireless Fidelity*
Bezdrátová síť

UWB *Ultra-Wideband*
Širokopásmová komunikační technologie

FireWire Rozhraní pro připojení zařízení k PC

USB *universal serial bus*
Rozhraní pro připojení zařízení k PC

BER *bit error rate*
bitová chybovost výkonu

ID *identification*
identifikace

SIM *Simple Instant Messenger*
Jednoduchý komunikační klient

MPEG *Motion Pictures Expert Group*
Skupina expertů na pohyblivé obrázky – kódovací formát pro video

AAC *Advanced Audio Code*
Pokročilé zvukové kódování

ISDN *Integrated Services Digital Network*
Integrovaný digitální síťový systém

WAP *Wireless Access Protocol*
Bezdrátový přístupový protokol

FTP *file Transfer Protocol*
Protokol pro přenos souborů

RSSI *Remote Signal Strenght Indication*
Kontrolní signál indikace výkonu

GFSK *Gaussian Frequency Shift Keying*
Gausův frekvenční posunovací klíč

ALU *Arithmetic Logic Unit*
Aritmeticko logická jednotka

RISC *Reduced Instruction Set Computer*
počítač s redukovaným souborem instrukcí

Úvod

Bezdrátová komunikace je v dnešní době velmi používaný způsob pro ovládání a komunikaci různých zařízení i technologických procesů. Její obrovskou výhodou je, že nepotřebuje fyzické spojení s ostatními zařízeními ani přímou viditelnost, jak to bývá u jiných technologii. Ideální je vzhledem k poměru dosahu a spotřeby energie. Ohromující je i její možnost miniaturizace a velkou výhodou je propracovaná vnitřní struktura, usnadňující používání v mnoha oborech i rozmanitých zařízeních. Rozšíření použití pomáhá zjednodušovat a usnadňovat život a práci lidí.

Cílem této bakalářské práce je seznámit se s principem fungování a způsobem komunikace Bluetooth. Vysvětlit, jak probíhá komunikace mezi Bluetooth zařízeními a jakým způsobem se tvoří a fungují Bluetooth sítě. Dobré porozumění struktuře Bluetooth jednotky a významu jednotlivých komunikačních vrstev je základem pro návrh hardwaru a softwaru.

Výslednou prací by měl být návrh a sestavení funkčního zařízení pro sběr dat a komunikaci prostřednictvím Bluetooth modulu. Pro ověření správnosti fungování by měla být vytvořena jednoduchá testovací aplikace s použitím PDA zařízení. Měřením spojení Bluetooth modulu a PDA by se měla zjistit propustnost komunikačního kanálu.

Obrázek 0.1 – znak Bluetooth

1. Historie bluetooth

Příběh vývoje a vzniku Bluetooth je opravdu zajímavý. Zahrnuje vikingského krále z desátého století, přes holandsko-švédskou skupinu inženýrů až po mezinárodní společenství vysoce technicky vyspělých společností. A to vše jen díky tomu, že kdosi kdesi chtěl odstranit malý, tenký drátek mezi svým telefonem a sluchátkem s mikrofonem.

1.1. Vývoj a historie bluetooth

Název technologie je odvozen od přezdívky dánského krále Haralda II – Blltand, který měl velkou schopnost spojovat země a lidi. Během 10. století sjednotil skandinávský lid. Také technologie Bluetooth má za cíl sjednotit osobní komunikační a výpočetní zařízení. "Bluetooth" (nebo Blaltand, v dánštině) nemá nic společného s Haraldovou barvou zubů, naopak to vzniklo v souvislosti s jeho neobvykle tmavou pletí a jeho velmi tmavými vlasy. Slovní spojení "Blltand" je zřejmě odvozený z dvou starých dánských slov, "bll" – snědý, tmavý a "tand" znamenající ohromný muž. Jméno technologie, původně zvolené pouze dočasně, nakonec zůstalo, a tak se dostalo i do povědomí uživatelů. Vývojem Bluetooth se zabývá od roku 1998 Bluetooth SIG (Special Industry Group), kterou jako neziskové průmyslové sdružení založily firmy Ericsson, IBM, Intel, Nokia a Toshiba. SIG slouží jako fórum pro rozvíjení a zvyšování Bluetooth specifikace, a jako primární nástroj pro tvorbu tržního uvědomění a celosvětové propagace technologie. Společný cíl všech Bluetooth SIG členů je způsobit převrat v osobní a obchodní oblasti pomocí mobilních zařízení - prosazováním všudypřítomné Bluetooth radiotechniky. Dnes má společnost přes 4000 členů. Mezi nejvýznamnější prosazovatele Bluetooth - coby levné bezdrátové technologie s krátkým dosahem - dnes patří vedle zakladatelů SIG společnosti 3Com, Agere, Microsoft a Motorola.

Modré logo vzniklo složením dvou písmenek H (zobrazeno jako hvězdička „X“) a B podle Harald Bluetooth [1] [4] [5]

Obrázek 1.1 – logo Bluetooth

1.2. Verze Bluetooth

V současnosti byla již vydána verze Bluetooth 2.0 , přesto většina dostupných přístrojů zatím používá verzi 1.1 nebo 1.2. Tyto verze však trpí řadou „dětských nemocí“, což má za následek nedůvěru v tuto techniku (řada chyb programového vybavení, nekompatibilita přístrojů různých výrobců apod.).

Novinkou verze 1.2 je vylepšená skoková změna kmitočtů AFH zmenšující interference s jinými rádiovými technikami. Bluetooth 1.2 nabízí vylepšenou detekci přenosových chyb. Standardní verze 1.1 a 1.2 jsou kompatibilní. Verze 1.2 však není rychlejší. [2]

1.3. Budoucí vývoj Bluetooth

Popularita Bluetooth zařízení stále roste. Ukazují to nejen statistická čísla, ale i samotný prodej. Bluetooth radiotechnika je jednou z nejpoužívanějších hned po GSM a Wi-fi. Bluetooth technologie pronikla do všech možných oblastí techniky, jako mobilní telefony, auta, MP3 přehrávače, osobní digitální asistenti (PDA) a mnoho dalších zařízení.

Organizace zaštiťující technologii Bluetooth dokončuje specifikaci další generace tohoto bezdrátového standardu pod označením Seattle. Důraz bude kladen především na rychlost, která má zajistit bezproblémový přenos videa ve vysokém rozlišení či velkých souborů mezi různými zařízeními. Hovoří až o rychlostech kolem 500 Mbit/s na 2m a 110 Mbit/s na 10m.

Pomoci k tomu má širokopásmová technologie UWB (ultra-wideband), kterou vyvinula skupina firem sdružená v WiMedia Alliance. Patří sem například Hewlett-Packard, Microsoft, Intel a další.

Technologie UWB (ultraširoké pásmo) se připravuje pro komunikaci rychlostí od 480 Mb/s na krátké vzdálenosti v pásmu 3,1 až 10,6 GHz. Firmy, které na ní pracují, již dříve slíbily bezdrátovou náhradu technologií USB a FireWire (FireWireless, Wireless 1394, IEEE1394c), což má samozřejmě vliv i na Bluetooth.

Hlavní změnou v novém Bluetooth tak má být zvýšení přenosové rychlosti a přidání dalších přenosových fyzických vrstev k Bluetooth. Dosah má být okolo 100 metrů a spotřeba bude srovnatelná se současnými Bluetooth systémy.

Velkým problémem se může stát 6GHz pásmo, ve kterém bude nové Bluetooth provozováno. V řadě zemí je totiž licencované, a to znamená, že pro jeho využívání je potřeba speciální povolení.

Vývoj Bluetooth čipů

Společnost Broadcom připravuje nové čipy určené pro mobily, PDA, komunikátory a multimediální přehrávače. Tyto čipy mají integrovaný modul Bluetooth 2.0, resp. 2.1 a navíc i velmi citlivý FM tuner. Jsou lákavé pro výrobce mobilních přístrojů, protože vyžadují asi 1/3 místa, které zabírají současné FM tunery a i cenově jsou na tom příznivěji. Celková plocha čipu je menší než 35 mm^2.

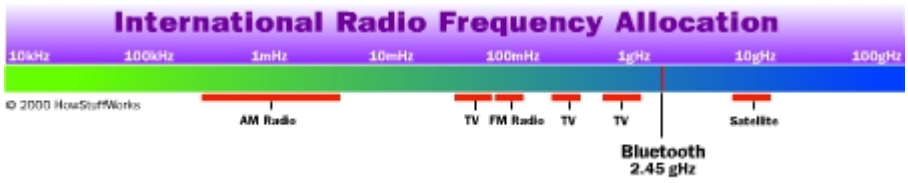
Obrázek 1.2 – Bluetooth chip s FM rádiem

2. Princip fungování

2.1. Specifikace Bluetooth 1.1

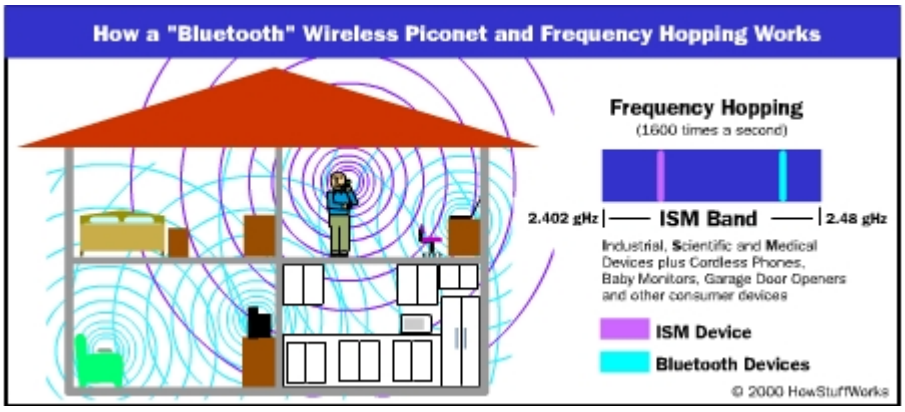
Specifikace Bluetooth (první verze byla k dispozici v roce 1999) je charakteristická nízkými nároky na napájení a spoluprací s malými koncovými zařízeními.

Rychlost na fyzické vrstvě dosahuje 1 Mbit/s, přičemž skutečná propustnost dat se pohybuje maximálně kolem 720 kbit/s. Komunikace po Bluetooth nabízí až tři hlasové kanály. Bluetooth pracuje podobně jako WLAN 802.11b v bezlicenčním pásmu 2,4 GHz.



Obrázek 2.1 – Frekvenční spektrum světového rádiového vysílání

Na rozdíl od 802.11b ale Bluetooth využívá metody rozprostřeného spektra s přeskakováním kmitočtů (Frequency Hopping Spread Spectrum, FHSS), kdy rádiový signál velmi rychle (1600krát za sekundu) náhodně přeskakuje mezi 79 jedno-MHz kanály.



Obrázek 2.2 – Rozsah a přeskoková frekvence Bluetooth

Veškerou komunikaci v síti Bluetooth řídí hlavní stanice (master) prostřednictvím protokolu výzvy. Podřízená stanice (slave) může komunikovat s ostatními výhradně prostřednictvím hlavní stanice.

Komunikace mezi hlavní stanicí a podřízenou stanicí je asynchronní bez spojení (asynchronous connectionless). Hlavní stanice alokuje časové úseky podle potřeb pro každý typ komunikace (synchronní nebo asynchronní) prostřednictvím mnohonásobného přístupu s časovým dělením (Time Division Multiple Access, TDMA).

Bluetooth používá stejné kmitočty pro vysílání a příjem s využitím Time Division Duplexing (TDD), které také umožňuje, aby jedna stanice sítě byla současně podřízenou i hlavní stanicí.

Umožňuje různorodé služby prostřednictvím zabudované podpory kvality služeb (Quality of Service, QoS).

Bluetooth volitelně nabízí až tři hlasové kanály o 64 kbit/s (tento volitelný typ spojení je synchronní se spojením, synchronous connection-oriented).

Pro zabezpečení používá stejný protokol jako WLAN, protokol WEP (Wired Equivalent Privacy), ale s 128bitovým klíčem.

Malý dosah sítě řádově do deseti metrů je s ohledem na bezpečnost velkou výhodou ve srovnání se sítěmi 802.11, kde se lze do sítě nabourat až stovky metrů daleko. [3]

2.1.1. Vylepšení pro specifikaci bluetooth 1.2

Další verze specifikace Bluetooth 1.2 schválená v roce 2003 je zakomponována do normy 802.15.1a. Je slučitelná s předchozí verzí 1.1. Dočkala se vylepšení jako je Adaptive Frequency Hopping (adaptivní střídání frekvencí): Bluetooth periodicky střídá frekvenci, na které vysílá a přijímá data. Dle standardu 1.2 vynechává kanály, na kterých již vysílá někdo jiný.

Potlačení hluku a ozvěny umožňuje zjednodušit elektroniku v handsfree, což je užitečné v každodenním provozu.

Quality of Service (QoS, kvalita služby): Zatímco datový provoz často může počkat a uživateli nebude vadit zlomek sekundy zpoždění při přenosu e-mailu či obrázku z digitálního fotoaparátu, hlasový přenos nečeká a zpoždění dat znamená výpadek. Proto

bylo nutno QoS uspokojivě vyřešit, díky tomu mohly vzniknout kvalitní bezdrátová sluchátka pro domácí stereo.

Anonymní mód: Podobně jako síťová karta v počítači nebo adaptér pro Wi-Fi i Bluetooth vysílá do éteru výrobní číslo adaptéru coby fyzickou adresu zařízení. Nově zavedený anonymní mód umožňuje fyzickou adresu skrýt.

„Pětiminutové pravidlo“: Novému uživateli by mělo zapojení a zprovoznění nového bluetoothového zařízení trvat jen pět minut.

Dalším vylepšením jsou výkonové třídy. Podle výstupního výkonu se Bluetooth zařízení dělí do 3 tříd:

Výkonová třída	Max. výstupní výkon	Max. vzdálenost
Třída 1	100 mW (20 dBm)	100 m
Třída 2	2,5 mW (4 dBm)	10 m
Třída 3	1 mW (0 dBm)	1 m

tabulka 2.1 – Tabulka výkonových tříd a vzdáleností

2.1.2. Bluetooth Specifikace 2.0

Verze specifikace má hned několik zásadních vylepšení oproti verzi 1.1 a 1.2. Pro verzi 2.0 je přichystán dosah až 100m i pro nižší výkonové třídy, což umožňuje snadnější použití pro rozsáhlejší prostory. Nová verze 2.0 s rozšířením EDR (Enhanced Data Rate) zdokonalenou rychlostí přenosu dat, nabídne 3 krát rychlejší přenosovou rychlost (až 10 krát v jistých případech) oproti verzi 1.2, tedy až 3 Mb/s se současným snížením příkonu díky redukci pracovního cyklu a zvýšením bezpečnosti. Výrazně byla vylepšená i práce více profilů najednou. Dočkala se též zvýšení počtu připojených zařízení v sítích ad-hoc, místo 8 aktivních je nyní možné připojit až 256 aktivních zařízení, to vše díky dostupnosti širšího pásma. Verze 2.0 se může pochlubit i zlepšeným BER - bitová chybovost výkonu.

Bluetooth 2.0 je doplněno o tzv. multicast, což umožňuje odesílat jednu zprávu na více zařízení naráz. Rozšíření soukromí znemožňuje detekovat zařízení v non-discoverable režimu.

V poslední řadě je zaručena i neméně důležitá zpětná kompatibilita s předchozími verzemi.

2.1.3. Bluetooth a UWB

Společnost Bluetooth SIG se rozhodla spojit svoje síly s Ultra-wideband známou jako UWB (širokopásmový přenos dat) Oběma společnostem to přináší výhody a možná i některé problém, které společně řeší.

Díky tomuto spojení bude Bluetooth schopno udržet krok s ostatními konkurenčními technologiemi a zároveň uživatelům poskytovat svoje přednosti jako je, malý výkon, nízká cena a propracovaná struktura jednotky a ad-hoc sítí.

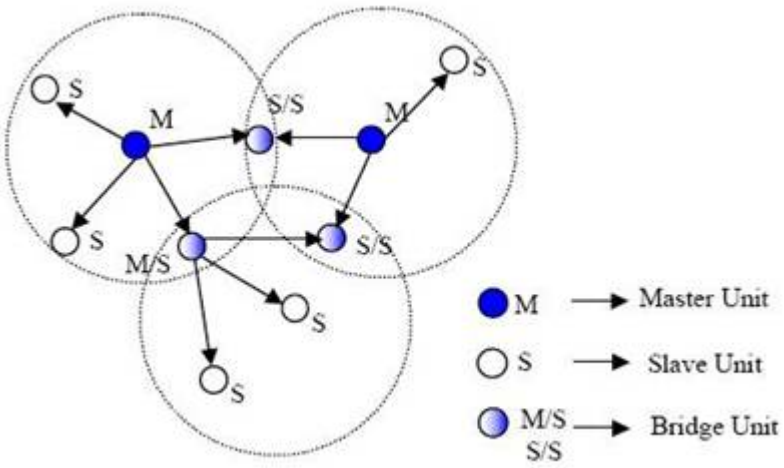
UWB získá část slávy dobyté Bluetooth, kvalitu značky, její tržní průbojnost, technickou a organizační zralost. Technologie UWB může skákat mnohokrát rychleji, než Bluetooth a tím dosahuje i větších rychlostí. Podařilo se již vytvořit demonstrační vrstvu s UWB, která dosahuje rychlosti 480Mbps. Oproti dnešním 3Mbps je to velký rychlostní skok. Výhled do budoucna je až na přenosovou rychlost 1Gbps. [4]

2.2. Topologie sítí Bluetooth

Standard Bluetooth umožňuje vytvářet tzv. pikosítě (piconet). V jedné síti mohou být minimálně dva přístroje (např. mobilní telefon a notebook), což představuje vlastně spojení od bodu k bodu. Pikosíť je možné kdykoli zvětšit a zmenšit, a vytvářet tak rychle se měnící sítě ad-hoc. Tyto sítě nemají předem stanovenou strukturu, vznikají za chodu podle toho kde se jednotlivé uzly budoucí sítě nalézají. Někdy je struktura závislá na náhodě, neboť algoritmy pro stavbu takových sítí využívají náhodná čísla při určování role uzlů. Ad-hoc sítě vznikají za chodu, distribuovaně nebo řízeny centrálními uzly. Po každém zapnutí se znovu samostatně konfigurují.

2.2.1. Obecné fungování pikosítě

Obvykle je pikosíť tvořena osmi stanicemi, z nichž jedna je nadřazená (master) a ostatní jsou podřízené (slave). Tyto podřízené (slave) uzly komunikují pouze s nadřazeným uzlem (master). Každý uzel může mít více rolí a tím pádem může být ve více pikosítích. Povolené kombinace jsou master-slave a slave-slave. Někdy se takovýmto uzlům říká bridge. Až deset pikosítí tvoří scatternet (rozložená síť), umožňuje pružnější komunikaci, v níž mohou vzájemně komunikovat všichni účastníci.



Obrázek 2.3 – Síť scatternet se všemi možnými rolemi uzlů

Rozsáhlejší pikosíť obsahuje až 255 účastníků, přičemž v jednom okamžiku může být aktivních osm přístrojů. Ostatní přístroje jsou v tzv. parked režimu (spící režim). S těmito uzly se komunikuje pouze občas. Pokud chce nějaký parked uzel začít komunikovat s master uzlem, je nutné jej převést do connected režimu.(spojovací režim) Pro zachování max. 7 aktivních slave uzlů je nutné jiný uzel převést do stavu park.

Pro zvýšení počtu aktivních přístrojů Bluetooth jsou nasazovány přístupové body BAP, kterými lze vybudovat další pikosítě, které se mohou i překrývat (a to i v okruhu 10 m). Přístupové body mohou spojovat systém Bluetooth se stávajícími lokálními sítěmi LAN, a tvoří tak jejich bezdrátové zakončení směrem k uživateli. V místnostech mohou být umístěny jak na stropě, tak i ve zdi (podobně jako elektrické zásuvky). Pro vybavení například celé budovy technikou Bluetooth je zapotřebí několika BAP, spojených obvykle sítí Ethernet. [2]

Obrázek 2.4 – Příklad picodítě

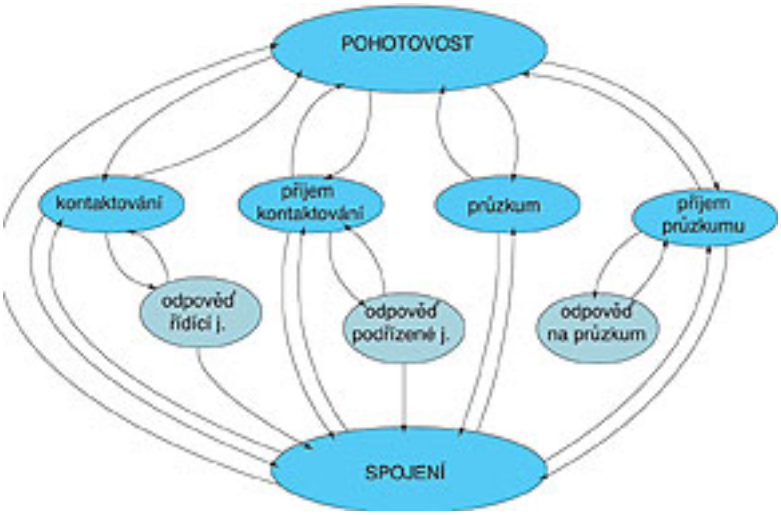
2.2.2. Jednotlivé stavy uzlů

Pro komunikaci se v piconet síti používá přeskakování po jednotlivých kanálech. Tato sekvence je odvozena od Global ID adresy master uzlu a posunu (offset). Všechny slave uzly proto potřebují znát tyto dva údaje. Navíc je z tohoto patrné, že master uzel nemůže být masterem ve dvou sítích, protože by tyto sítě měli stejnou přeskakovací posloupnost.

Uzel v síti Bluetooth prochází několika stavy. Dají se rozdělit do tří skupin. Zaprvé je to stav připojen Standby (pohotovostní), kdy je uzel zapnutý. V tomto stavu fungují pouze vnitřní hodiny a jednotka má minimální spotřebu energie.

Pak jsou to stavy ve fázi připojování a to Inquiry (průzkum) a Inquiry scan (příjem průzkumu). Tyto dva procesy probíhají na omezeném počtu kanálů (32 rovnoměrně rozložených kanálů), slouží k objevení dvou zařízení navzájem. Během stavu Inquiry (průzkum) prozkoumávající jednotka sbírá adresy a hodnoty vnitřních hodin odpovídajících jednotek, které se nacházejí v jejím okolí. Poté je možno s kteroukoli z takto objevených jednotek navázat spojení pomocí procedury Page (kontaktování). Prozkoumávající jednotka průběžně vysílá průzkumnou zprávu prostřednictvím paketu ID na různých přeskokových frekvencích. Page (kontaktování) a Page Scan (příjem kontaktování), slouží k vytvoření spojení v rámci piconet. Uzel ve stavu Page odesílá opět na 32 kanálech Global ID uzlu, které chce připojit do sítě. Na to uzel odpovídá a předává opět své Global ID a ofset. Uzel ve stavu Page tyto informace zakomponuje do přeskakovací posloupnosti a je schopen přijímat a vysílat

Ve fázi připojení pak stavy Connect (připojit). Po úspěšném spojení získá uzel 3-bitovou adresu AMA (Active Member Address) v rámci sítě piconet – odtud omezení na 7 slave uzlů. Master má vždy adresu AMA rovnu 0. Stav Hold (uspání) a Sniff (probuzení) umožňuje „uspání“ uzlu a „probuzení“ vždy po určitém časovém intervalu. To jednak umožňuje šetřit energií a také omezí vysílání uzlu. Ten může vysílat jen ve „vzbuzeném“ stavu. Stav Park slouží k odstavení uzlu, pokud chceme k piconetu připojit více než 7 slave uzlů. Uzel získa 8-bitovou PMA (Parked Member Address), podle které je poté identifikován. Komunikace s parked uzlem probíhá v tzv. Beacon intervalech, které mohou trvat 1 nebo více časových slotů.



Obrázek 2.5 – Stavy uzlů v síti Bluetooth

2.2.3. Problematika vytváření Bluetooth sítí

Prvním faktorem je vzdálenost. Jelikož vysílací vzdálenost je 10 metrů, znamená to, že jedna pikosíť nemůže mít uzly slave vzdáleny více než 20 metrů. Může se tedy stát, že některé uzly se navzájem neuslyší. Tento fakt může být ne jen mezi uzly v jedné pikosíti ale i mezi uzly v rámci celého scatternetu. Takovým, kde je nutné při komunikaci mezi vzdálenými uzly použít prostředníka/y, se říká multi-hop sítě . Sítě, ve kterých může každý uzel slyšet každého souseda se říká single-hop. Je nasnadě, že v reálu se častěji objevují multi-hop sítě, neboť vzdálenost 10 metrů je malá pro rozsáhlejší sítě. Pro simulaci a tvorbu algoritmů je zase jednodušší uvažovat o single-hop sítích, neboť odpadnou problémy právě s neslyšitelností.

Algoritmy, které se zabývají výstavbou ad-hoc sítí se snaží optimalizovat několik, občas protichůdných, parametrů. Jsou jimi malý průměr sítě a malý počet skoků. Tyto parametry jsou důležité pro zpoždění dat při přenosu a zaručení této doby (QoS). Na druhou stranu je třeba minimalizovat vyzářený výkon. Jelikož vyzářený výkon roste se dosaženou vzdáleností kvadraticky, může být někdy výhodné provést více skoků a ušetřit tak energii. Dalším parametrem je minimalizace počtu pikosíti, případně zrušení cyklů. Tím nedochází ke zpoždění v důsledku přepínání a synchronizace bridge uzlů (master-slave, slave-slave) mezi sítěmi. Takto vzniklé sítě ale trpí na výpadky nebo rozpojení v důsledku vypnutí nějakého uzlu, protože neobsahují záložní cesty. Další výzvou pro algoritmy, resp. sítě, je flexibilita. Sítě se často mění, jednotlivé uzly mohou měnit svoji pozici a může se stát, že se dostanou z dosahu původní picosítě a připojí se k jiné. Zde by

mělo dojít k automatickému přeformování sítě. Vytvořená síť by měla mít vhodné vlastnosti pro routování. Dnes již technicky zvládnutými problémy je, aby síť byla úplně propojena, tj. všechny uzly mohli mezi sebou komunikovat a většina algoritmů se snaží zabránit nutnosti převádět uzly do stavu Parked při vytváření sítě. [4]

2.3. Profily Bluetooth

Přístroje standardu Bluetooth jsou vybaveny softwarovými profily pro různé způsoby využití. Jednotlivé aplikace vytváří příslušné profily. Je standardizováno přes dvacet profilů, např. pro budování sítí, pro přenos dat, zvuku či obrazu, pro tisk, pro přístup na kartu SIM mobilního telefonu nebo pro služby faxu. Komunikující přístroje musí mít stejný profil. V počátcích zavádění standardu Bluetooth chyběla standardizace právě těchto profilů, takže si každý z výrobců vytvořil vlastní profil a tím docházelo k neslučitelnosti přístrojů a k nedůvěře zákazníků v tuto novou bezdrátovou techniku.

2.3.1. Základní Profily

Každá profilová specifikace musí obsahovat následující základní informace:

- Závislosti na jiných profilech
- Návrh formátu uživatelského rozhraní
- Specifické části vrstev protokolů Bluetooth užívané příslušným profilem. Některé profily využívají určité volby a parametry nižších vrstev v Bluetooth protokolu, potom je nutné načíst některé servisní záznamy.

Základních profilů je zhruba dvacet, pro představu popis pár nejčastějších a nejdůležitějších:

Pokročilý audio distribuční profil (Advanced Audio Distribution Profile - A2DP)

Protokol řeší jak přenést kvalitní stereo zvuk mezi zařízením a mobilní částí. Ku příkladu třeba hudební přehrávač a sluchátka, mobil a hands-free, přičemž zdrojem je hudební přehrávač a zvukový interpret bezdrátové sluchátko s mikrofonem. A2DP definuje protokoly a procedury které realizují přenos kvalitního mono nebo stereo zvukového obsahu na ACL kanály. Tento profil se opírá o GAVDP (Všeobecný zvukový/obrazový distribuční profil). Zahrnuje v sobě povinnou podporu pro dílčí kódové pásmo (SBC) a podporuje volitelné zvukové formáty MPEG - 1,2 MPEG - 2,4 pro AAC.

Na dálku řízený zvukový/obrazový profil (Audio/Video Control Transport Protocol – AVRCP)

AVRCPIS je navržen k tomu, aby poskytoval standardní rozhraní pro vysokofrekvenční ovládání dálkových zařízení, jako je například televizní ovladač a mnoho dalších zařízení. Definuje jak ovládat charakteristické rysy dálkového ovládání jako je hlasitost, přepínání kanálů, nahrávání a další podobné funkce.

Základní zobrazovací profil (Basic Imaging Profile - BIP)

BIP definuje profil pomocí něhož můžeme nějaké zobrazovací zařízení dálkově řídit, ukládat jeho obraz, tisknout, či archívovat obraz. V BIP je také zahrnuta funkce pro převod formátu obrazu vhodného pro dané zařízení. Typické použití tohoto profilu je například dálkové ovládání kamery u mobilního telefonu.

Základní profil pro tisk (Basic Printing Profile - BPP)

Umožňuje zařízením posílat texty, e-maily, obrázky a další tiskové práce na tiskárnu. Profil BPP definuje dvě role, odesílatel a tiskárna. Klasickým příkladem je tisk z mobilního telefonu či PDA.

Běžný přístupový profil ISDN (Common ISDN Access Profile - CIP)

CIP definuje jakým způsobem se přenáší ISDN spojení přes bezdrátové spojení Bluetooth. Poskytuje neomezený přístup k datům a informacím stejně jako klasické ISDN spojení.

Profil vytáčeného telefonního připojení spolu s bezdrátovým přístupem

Definují spojení mobilního telefonu a jiného zařízení a způsob zpřístupnění telefonních služeb třeba internetu, wapu, vytáčené služby a další.

Profil pro přenos souborů (File Transfer Profile - FTP)

Profil FTP umožňuje přístup k souborům a složkám na serverech. FTP profil zahrnuje podporu ukládání, čtení a mazání souborů na serveru.

Všeobecný přístupový profil (Generic Access Profile - GAP)

Profil GAP poskytuje základy pro všechny ostatní profily a definuje základní parametry a způsoby pro spojení mezi Bluetooth zařízeními. Profil definuje:

- implementaci profilu GAP ve všech zařízeních
- všeobecné procedury pro objevování a navazování spojení se zařízeními
- základní terminologii uživatelského rozhraní

Výhodou je pro programátory při tvorbě nových profilů, mohou se odkazovat na základní funkce poskytované GAP profilem. Zabezpečuje výměnu základních informací mezi různými zařízeními.

Hands-Free profil (Hands-Free Profile - HFP)

Popisuje jak může hands-free zařízení navazovat a přijímat hovor. Klasickým příkladem může být používání mobilního telefonu v autě.

Osobní síťový profil (Personal Area Networking Profile - PAN)

PAN popisuje jak dva nebo více zařízení můžou vytvářet at-hot sítě a jak skrze stejný mechanizmus lze zpřístupnit i vzdálenou síť přes síťové připojení.

Profil služby objevení (Service Discovery Protocol SDP)

SDP se stará o rozpoznání poskytovaných služeb na dosažitelném serveru služeb. Také se stará o poskytování nových služeb při spojení se serverem. SDP může být v roli serveru poskytujícího služby nebo klienta. Server si udržuje databázi, kde si zaznamenává všechny podporované služby pro dané zařízení.

SIM přístupový profil (SIM Access Profile - SAP)

SAP dovolí zařízením jako auto-telefony postavené na GSM přístrojích se připojit k SIM kartě pomocí Bluetooth.

Profil sériového rozhraní počítače (Serial Port Profile - SPP)

SPP definuje spojní přes virtuální sériovou linku s počítačem a spojení dvou Bluetooth zařízení. Tento profil podporuje přenosovou rychlost dat 128 kbit/sec.

Synchronizační profil (Synchronization Profile - SYNC)

Synchronizační profil užívaný spolu s GOEP umožňuje synchronizaci kalendáře a adresové informace (osobní informační manažerské položky)mezi Bluetooth zařízeními. Profil také podporuje automatickou synchronizaci. Cílem tohoto profilu je výměna dat mezi počítačem a PDA. Definuje klienta se serverem a jejich synchronizační přístrojové role.

WAP přes Bluetooth Profil (WAP Over Bluetooth Profile - WAP)

WAP definuje spojení aplikační protokolové vrstvy s bezdrátovou technologii Bluetooth. Typické použití je mobilní telefon spojující Bluetooth se službou WAP. [4]

3. Technické parametry

3.1. Vysílací výkonové úrovně

Bluetooth zařízení funguje zároveň jako vysílač a přijímač, jehož výkonové úrovně jsou vztahovány k anténnímu konektoru. Bluetooth pracuje v bezlicenčním pásmu 2,4GHz. Zařízení v tomto pásmu musí dodržovat určitá pravidla. Jedním z pravidel je dodržení maximálního výstupního výkonu 100mW. Podle něj se zařízení dělí na jednotlivé třídy. Nejběžněji se používá druhá výkonová třída.

Výkonové třídy	Maximální výstupní výkon	Nominální výstupní výkon	Minimální výstupní výkon	Dosah
1	100 mW (20 dBm)	-	1 mW (0 dBm)	100m
2	2,5 mW (4 dBm)	1 mW (0 dBm)	0,25 mW (-6 dBm)	10m
3	1 mW (0 dBm)	-	-	1m

tabulka 3.1 – Výkonové třídy systému Bluetooth

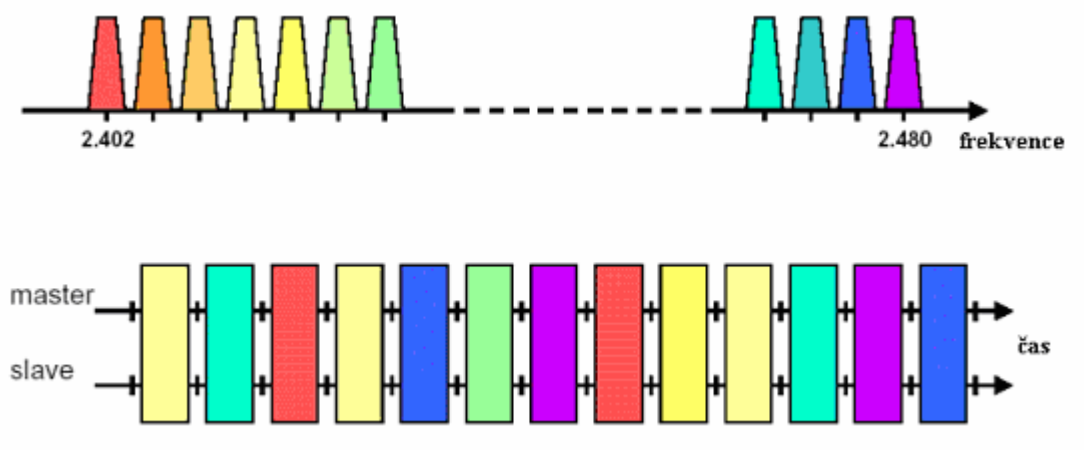
Minimální výstupní výkon PMIN je nepovinný. Může být volen dle požadavků aplikace. U zařízení první třídy je požadováno řízení výstupního výkonu, které je založeno na RSSI (Remote Signal Strenght Indication). Technologie Bluetooth používá zpětné zasílání požadavků na zvýšení či snížení výkonu. Řízení výkonu se realizuje po krocích, přičemž maximální velikost kroku je 8 dB a minimální je 2 dB. Optimalizace výstupního výkonu se provádí na základě informace v řídícím paketu.

3.2. Frekvenční pásma a rozdělení rádiových kanálů

Systém Bluetooth pracuje v nelicencovaném frekvenčním pásmu ISM (Industrial, Scientific, Medicine) na frekvenci 2,4 GHz. Šířka frekvenčního pásma pro Bluetooth zařízení v Evropě a ve většině ostatních zemích je 2400 - 2483,5 MHz. Pro nosné frekvence platí vztah

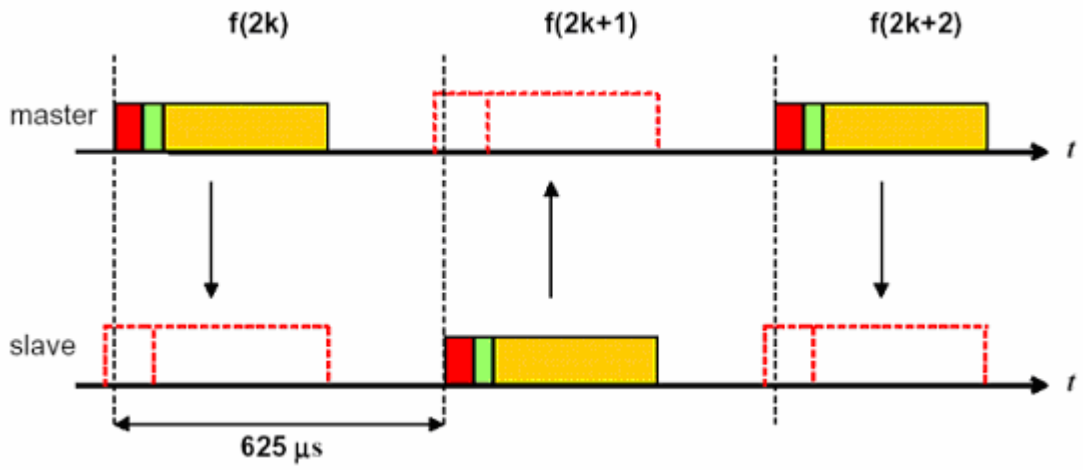
$$f = 2402 + k \text{ [MHz]}, \text{ kde } k = 0, ..., 78$$

V tomto frekvenčním pásmu je tedy k dispozici 79 rádiových kanálů. Šířka rádiového kanálu je 1 MHz. Mimo pásmo jsou definována tzv. ochranná pásma, aby byly dodrženy normy. Dolní ochranné pásmo má šířku 2 MHz, horní ochranné pásmo 3,5 MHz.



Obrázek 3.1 – Rozdělení pásma na jednotlivé frekvence

Přenosový kanál je rozdělen na time sloty, každý je vysílán na jiné frekvenci a má délku 625 ms. Bluetooth používá modulaci GFSK (Gaussian Frequency Shift Keying), kde log. 1 je reprezentována pozitivní frekvenční odchylkou, log. 0 negativní frekvenční odchylkou. Modulační přenosová rychlost je rovna 1Mbps.



Obrázek 3.2 – Princip komunikace v time slotech

Existuje také druhá varianta systému Bluetooth s šířkou frekvenčního pásma 2446,5 - 2483,5 MHz. Pro nosné frekvence platí vztah

$$f = 2454 + k \text{ [MHz]}, \text{ kde } k = 0, ..., 22$$

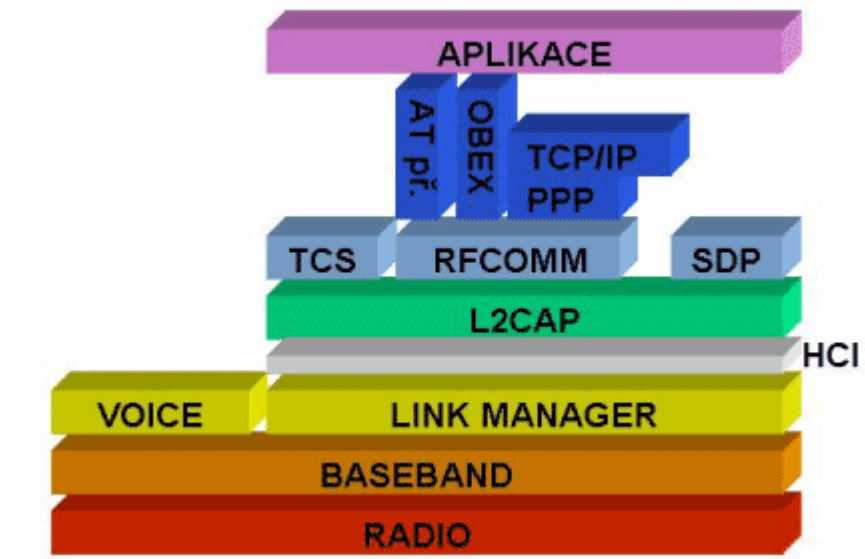
Šířka rádiového kanálu je opět 1 MHz. Dolní i horní ochranné pásmo je 7,5 MHz. S touto variantou se můžeme setkat například ve Francii a Španělsku. V těchto zemích nebylo možné vzhledem k národnímu přidělení kmitočtového pásma přijmout pro Bluetooth rozsah frekvencí podle původního plánu.

4. Struktura Bluetooth jednotky a vrstvy

4.1. Základní struktura Bluetooth jednotky

Systémy Bluetooth se rozdělují podle tří základních funkčních bloků:

- Bluetooth radio – vysílač, přijímač, analogová rádio-elektronika
- Bluetooth link controller (Baseband) – řízení spojení, komunikace, přístupu, identifikace
- Bluetooth link manager – příprava dat



Obrázek 4.1 – Jednotlivé vrstvy a jejich pozice

Vrstva HCI rozděluje strukturu jednotky na vyšší a nižší vrstvy. Z nižších vrstev to jsou:

Vrstva Bluetooth Radio

Tato vrstva leží v hierarchii nejníže. Charakterizuje použité frekvenční pásmo, organizaci kanálů, řízení vysílacího výkonu, použitou modulaci, demodulaci dat do RF(rádio frekvenčního) signálu pro přenos vzduchem. Poskytuje rozhraní pro anténu.

Baseband

Baseband je fyzickou vrstvou v Bluetooth, která leží hned nad Radio vrstvou. Na starosti má řízení fyzických kanálů a spojení, spolu s dalšími službami jako je oprava chyb, „hopping“ algoritmu, příprava dat, datové přenosy, zajištění hlasové a audio komunikace, datová bezpečnost, identifikace a šifrování. Baseband protokol je implementován jako Link Controler (kontrola linek), společně s Link managerem se stará o vytváření spojení a kontrolu výkonu. Data jsou přenášena duplexně v synchronním módu (SCO) určeném zejména pro hlasovou komunikaci ve třech kanálech s přenosovou rychlostí 64 kbit/s, nebo v asynchronním módu (ACL) s rychlostí pro nesymetrický přenos 721 kbit/s se zpětným kanálem 57,6 kbit/s, nebo 432,6 kbit/s v obou směrech pro symetrický přenos. Baseband vyžaduje časové dělení kanálů TDD (time division duplex), střídavé přijímání a vysílání dat.

Link Manager – LM

Link Manager zabezpečuje konfigurovaní linky, synchronizaci zařízení při vytváření spojení, ověření zařízení na základě privátních klíčů s využitím metody výzva-odezva, šifrování spojení , detekci a korekci chyb, řízení výkonu a mnohé další funkce. Vyhledává v okolí jiné zařízení a komunikuje s jejich Link Managerem prostřednictvím Link Manager Protocol (LMP) a vytváří spojení . Na vykonávání jím poskytovaných služeb LM používá služby vrstvy Link Controlleru. [13]

Host Controller Interface – HCI

HCI je rozhraní, které poskytuje uniformní přístup softwarové části protokolového zásobníku k fyzické části zařízení Bluetooth (hardware a firmware).

- HCI firmware - Nachází se v časti Bluetooth hardware. Implementuje HCI příkazy prostřednictvím příkazů Baseband a LM vrstvy, přístup k hardwarovým, stavovým a řídícím registrům a k registrům událostí.
- HCI driver - Nachází se v části Host (software). Zabezpečuje analýzu přijatých událostí, na základě kterých poskytuje informace vyšším vrstvám.

- Host Controller Transport Layer (Physical Bus Driver) - definuje několik různých způsobů komunikace: USB, UART a RS232. Tyto způsoby připojují hardwarové části Bluetooth zařízení k hlavnímu zařízení (HOST).

Logical Link Control and Adaptation Protocol - L2CAP

Jednoduchý protokol datového spoje patřící do vyšších vrstev, který poskytuje služby na přenos se spojením a bez spojení k vyšším vrstvám. L2CAP podporuje protokoly vyšších vrstev jako multiplexing protokolu (RFCOMM), segmentace a sestavování příkazů, deklarace kvality spojení QoS, a schopností práce se skupinami. Vyšší vrstvy a aplikační vrstva umožňuje L2CAP přijímat pakety až 64kB dlouhá uživatelská data a 16B CRC (kontrolní součet) ze základního pásma. Podporované jsou dva typy spojení synchronní (SCO) a asynchronní (ACL). L2CAP podporuje spojení pouze asynchronní spojení ACL, pro synchronní spojení SCO se podpora připravuje.

TCS – definice správy mobility, ovládání přenosu videa a dat

RFCOMM

Jednoduchý transportní protokol, který zastupuje RS232 obvod pro komunikaci s L2CAP. RFCOMM protokol podporuje až 60 simultánní spojení (RFCOMM kanály)mezi dvěma Bluetooth zařízeními.

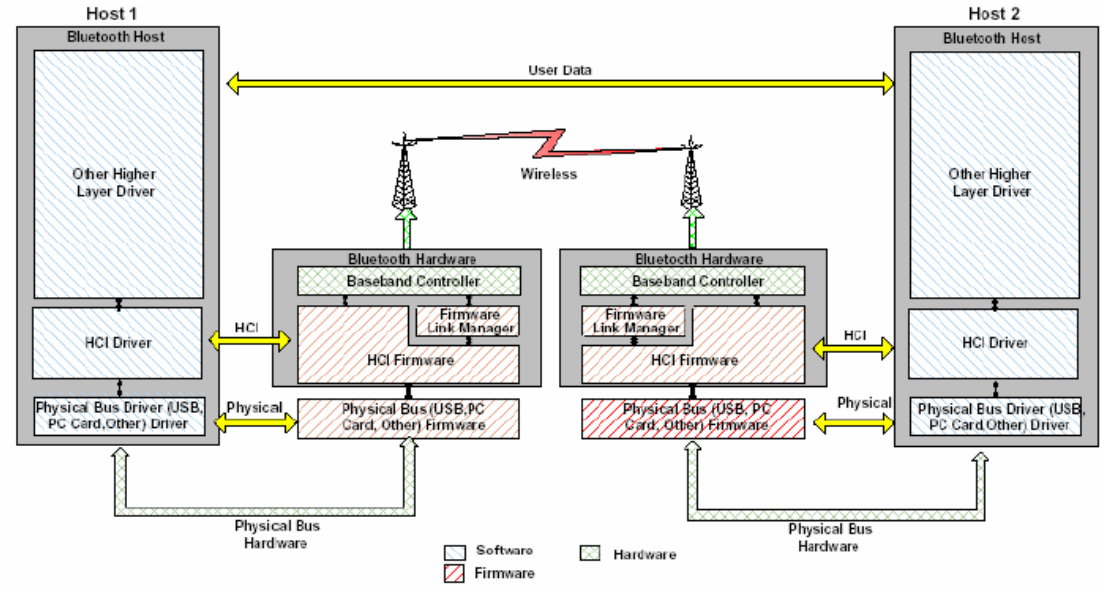
OBEX - je široce užívaný protokol pro jednoduché přesuny souboru mezi mobilními zařízeními.

Network Access with PPP (LAN) Profiles

Profil je postaven na RFCOMM a zajišťuje přístupový bod pro spojení do sítě LAN nebo spojení dvou počítačů (PPP).

Service Discovery Protocol - SDP

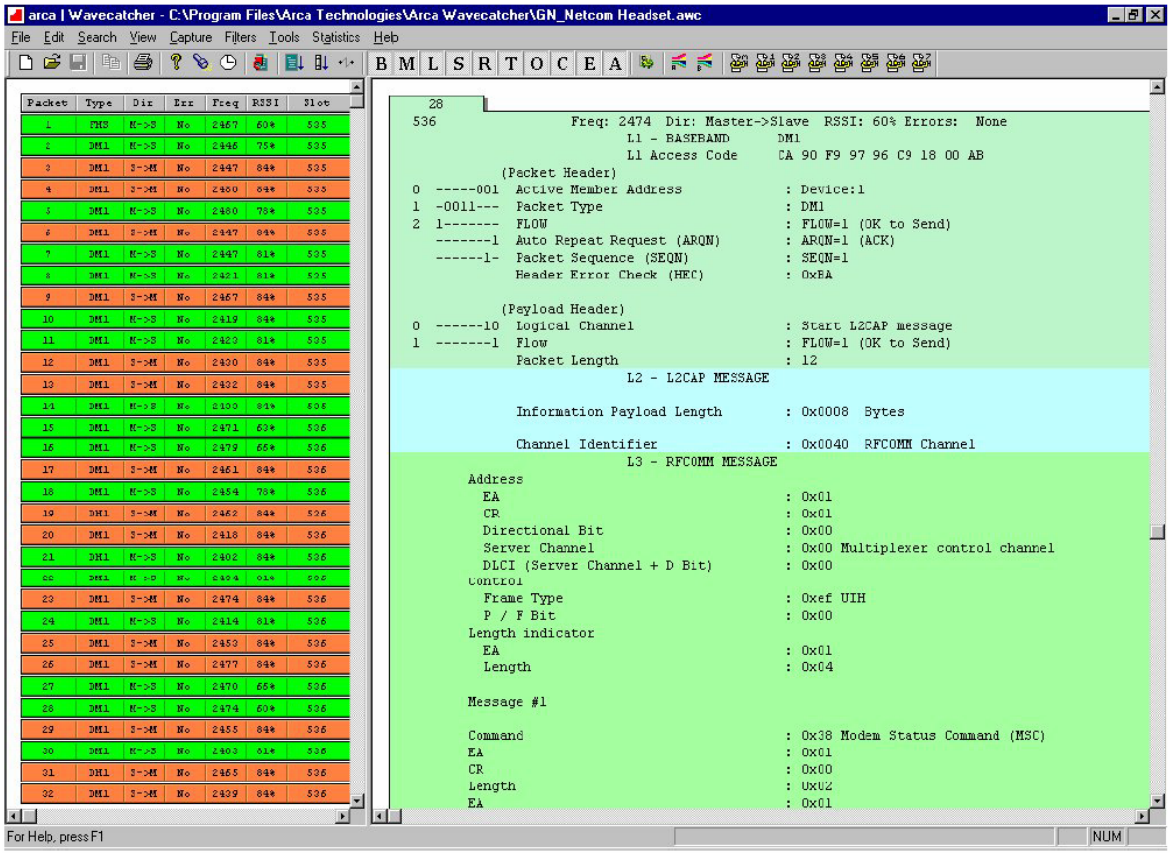
Protokol má za úkol odhalit aplikacím, které všechny služby mohou použít a jaké jsou vlastnosti těchto služeb. Služba je důležitá vzhledem k dynamice některých změn o kterých informuje jako kvalita spojení QoS závislé na vzdálenosti a další informace.



Obrázek 4.2 – příklad dvou zařízení komunikujících přes Bluetooth

4.2. Analýza přenosu dat

Bluetooth profilový simulátor firmy Arca dokáže velmi rychle a jednoduše generovat, testovat a analyzovat Bluetooth provoz (zastoupí i koncové zařízení). Jeho funkcí je zachycovat zprávy poslané mezi Bluetooth zařízeními, stahuje je a poskytuje detailní dekódování přenesených informací. Protokolový analyzátor analyzuje všechny základní Bluetooth protokoly. Tento přístroj se nejprve synchronizuje na zařízení Bluetooth, které je v módu master a pak monitoruje provoz. Je možno sledovat až 7 zařízení v módu slave. Po aktivaci jednotlivých BT zařízení, je nutné vygenerovat provoz (např.: přenos dat), poté je tento provoz analyzátorem zachycen. Konkrétním výstupem je pak podrobný výpis všech paketů uskutečněné komunikace, které je dále možno zkoumat na základě rozdělení do jednotlivých vrstev či protokolů. Lze vysledovat statické informace přenosu, jako např. počet přenesených paketů, počet paketů různých protokolů nebo počet chybných paketů apod..[18]



Obrázek 4.3 – protokolový analyzátor přenesených dat Arca – Wawecatcher

5. Bezpečnost Bluetooth a hrozby

Bezdrátový svět v dnešní době znamená neviditelný přenos dat mezi jednotlivými zařízeními, zeměmi a lidmi. Tyto data, ve formě e-mailů, obrázků, kontaktů a adres, jsou pro každého z nás drahocenné a soukromé, proto potřebujeme tyto informace bezpečně doručit zamýšlenému příjemci, aniž by je získal kdokoli jiný. Bezdrátové standarty jsou po celém světě vyvíjeny tak, aby splňovaly bezpečnostní požadavky svých uživatelů a efektivně chránily před zneužitím soukromích informací. Stejný cíl má i bezdrátová technologie Bluetooth.

Bluetooth kladla velký důraz na bezpečnost již v samotných počátcích svého vývoje, díky tomu je Bluetooth spojení poměrně dosti bezpečné i když i v tomto případě se našlo pár cest jak obejít bezpečnostní algoritmy.

Bluetooth bezpečnost je postavena na třech důležitých službách: Oprávnění (Authorization), Ověření (Authentication), Kódování (Encryption). Služba ověření zařízení (Authentication) má na starosti zajistit, zda se nějaké jiné zařízení nesnaží podstrčit místo původního zařízení sebe. Služba oprávnění (Authorization) zkoumá, jestli danému zařízení je dovolen přístup k daným informacím nebo službám. Kódování (Encryption) má na starosti heslování informací, aby se je neoprávněně nedozvěděl někdo jiný.

V Bluetooth, ve všeobecném přístupovém profilu při komunikaci s jiným zařízením, jsou na výběr tři bezpečnostní režimy.

BR	Název režimu	Oprávnění Authorization	Ověření Authentication	Důvěryhodnost Confidentiality	Popis
1	*bez zabezpečení*	**Ne**	**Ne**	**Ne**	*Není implementována žádná ochrana*
2	*servisní úroveň zabezpečení*	**Ano**	**Ano**	**Ano**	*Přístup je povolen jen k jednotlivým službám*
3	*spojovací úroveň zabezpečení*	**Ne**	**Ano**	**Ano**	*Bezpečnost je vynucená pro všechny aplikace již na běžné úrovni na začátku spojení*

tabulka 5.1 – Bezpečnostní režimy Bluetooth

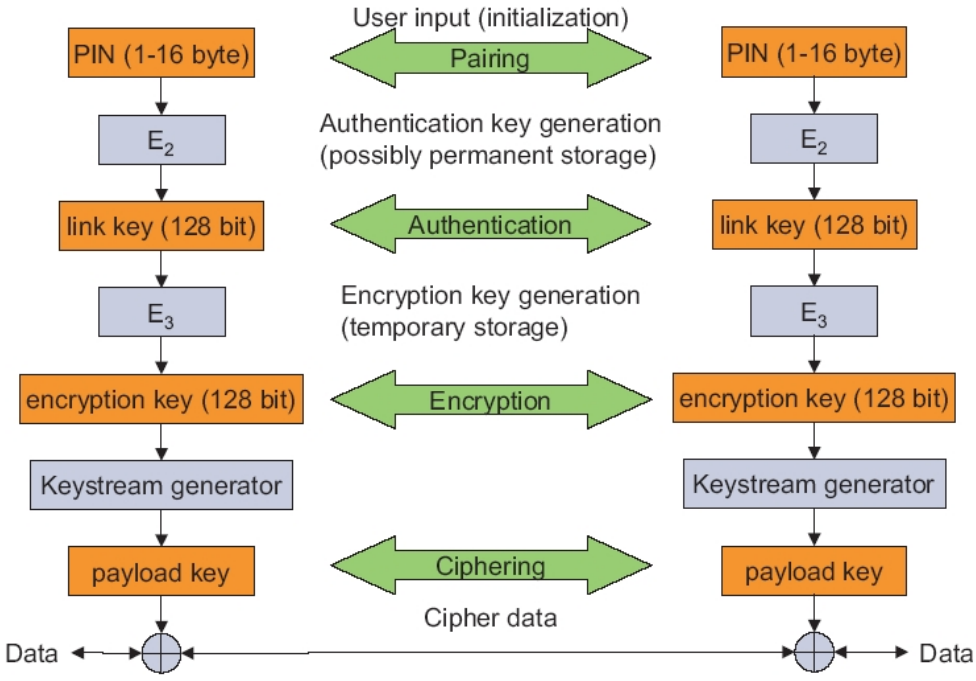
Každý výrobce si sám určuje bezpečnostní režim pro své výrobky.

Zařízení a služby mohou používat ještě další volby zabezpečení. Pro zařízení jsou to úrovně „Důvěryhodná zařízení“ a „Nedůvěryhodná zařízení“. Důvěryhodná zařízení mají při párování s druhým zařízením neomezený přístup ke všem službám onoho zařízení. Služby pro „Nedůvěryhodná zařízení“ mají ještě další tři úrovně zabezpečení:

BS	Oprávnění Authorization	Ověření Authentication	Kódování Encryption	Popis
1	**Ano**	**Ano**	**Ano**	*Služby, které požadují oprávnění a legalizaci*
2	**Ne**	**Ano**	**Ano**	*Služby, které požadují pouze legalizaci*
3	**Ne**	**Ne**	**Ano**	*Služby, které jsou otevřené pro všechny zařízení*

tabulka 5.2 – Bezpečnostní úrovně služeb

Bezpečnost Bluetooth je založená na generování klíčů za použití PIN kódu, který může být dlouhý 1 až 16 bajtů. Nejvíce zařízení používá 4-bajtový PIN kód. Nejprve algoritmus E2 vygeneruje 16 - bajtový spojovací klíč, pomocí PIN kódu a dalších čísel, jako je náhodné číslo a další. Kódovací klíč vznikne pomocí algoritmu E3 na základě spojovacího klíče z autorizačního procesu. Pomocí spojovacího klíče se uskutečňuje autorizační proces a pomocí kódovacího klíče je zajištěno šifrovaní přenosu.



Obrázek 5.1 – Navázání spojení dvou BT zařízení

Autorizační proces zahajuje zařízení, které zasílá žádost o spojení, posláním adresy (BD_ADDR). Adresa má délku 48-bitů a je jedinečná, podobně jako u síťových adaptérů s MAC adresou. Jako odpověď dostane 128-bitové náhodně vygenerované číslo. Obě zařízení následně vygenerují ověřovací odpověď z adresy BD_ADDR, spojovacího klíče a náhodného čísla druhého zařízení, což se nazývá SRES. Tento SRES si obě zařízení navzájem vymění a jsou-li shodná pokusí se tímto navázat spojení.

5.1. Nečastější známé mezery a útoky

Problém standardního nastavení

Jedním z problému bezpečnosti Bluetooth je fakt, že mnoho zařízení prodávajících se na běžném trhu mají nastavené standardní hodnoty pin kódu na 0000. V důsledku toho je zařízení standardně objevitelé a přijímá všechny příchozí soubory. Největší problém způsobuje standardní pin kód u zařízení s velmi omezenými možnostmi nastavení uživatelem, jako jsou Bluetooth sluchátka s mikrofonem. U těchto zařízení uživatelem nemá možnost nastavení jiného pin kódu, a tak se může stát obětí zlomyslného uživatele, který má možnost se s tímto zařízením spárovat. Naštěstí jsou dostupná řešení pro tento problém. Řeší se pomocí tlačítka, které dovolí párování se zařízením, pouze když je stisknuté a to jen po určitou dobu, třeba 30s. Případně je omezen počet párování například na jedno, nebo je povolené kdykoliv pouze jedno spojení.

Falešné jméno zařízení (Device name spoofing)

Mnoho Bluetooth zařízení neukazuje během párování celé jméno zařízení se kterým se páruje. Jestliže se zařízení A pokusí vytvořit pár s B, potom zařízení M může využívat stejné jméno jako zařízení B. Pokud M zaslechne přenos kódu mezi A a B, může se pokusit spárovat s A ještě před B a tak by se mohl nechat A zmást a spárovat se s M namísto B. Zatím co B bude zmateno, zařízení M má dost času na to zkusit další útok zařízení, například Zadní dveře (backdoor) nebo Bluebug.

Bluesnarfing (léčka)

Bluesnarfing útočníkovi dovolí získat přístup k některým, případně všem, informacím o cílovém zařízení. Tato zranitelnost je způsobena realizačními vadami. Útočník způsobí klasické přetečení zásobníku. Bluesnarfing může ovlivnit jen specifická

zařízení, týká se to především starších mobilních zařízení s prvotním Bluetooth (Nokia 6310i). Zařízení mají různou dostupnost informací, může to být telefonní seznam, kalendář, seznam úkolů a schůzek, soubory, obrazové soubory, IMEI (mezinárodní mobilní přístrojová identita). Po tomto útoku nejsou žádné stopy po útočníkovi ani žádné identifikační informace. Neúspěšné útoky často končí resetování zařízení. Útočník musí být v okruhu 10m, pokud nepoužívá specielní zařízení.

Bluejacking (cinknutí)

Bluejacking nezpůsobuje žádnou ztrátu dat ani služeb, ačkoli se přihodí velmi rychle a dosti často. Bluejacker se pokouší o navázání spojení použitím jména zařízení, například by jméno mohlo být "hezké tvídové kalhoty". Délka jména zařízení může být až 248 znaků. Danému zařízení pošle útočník navštívenku se svým jménem s úmyslem, aby druhá strana reagovala a povolila spárování. Pro provedení Bluejackingu musí být obě zařízení v okruhu 10m a navzájem se slyšet.

Zadní dveře (backdoor)

Tento tajný útok je velmi nebezpečný, protože o něm především uživatel vůbec nemusí vědět. Párování se uskuteční pomocí falešného jména zařízení (Device name spoofing) nebo jinou metodou a hned po spárování útočník odstraní párovací záznam z listu, což způsobí, že po spárování není vidět. Útočník tak může získat veškerá práva. Jedinou účinnou obranou je úplný restart zařízení. SIG doporučuje párování pokud možno mimo veřejné prostory a párovat jen je-li to opravdu nutné.

Bluebug (brouk)

Bluebuging umožňuje zkušeným jedincům zpřístupnit mobilní telefon pomocí příkazů používaných bezdrátovými Bluetooth technologiemi, aniž by se o tom mohl uživatel dozvědět. Útočník nepotřebuje být spárovaný s cílovým zařízením. Tento způsob útoku umožňuje útočníkovi uskutečňovat hovory, posílat a přijímat textové zprávy, kompletně pracovat s telefonním seznamem nebo odposlouchávat hovor, či připojit se k internetu. Tak jako při ostatních útocích musí být útočník v okruhu 10m, pokud nepoužívá specielní zařízení. Bluebuging je odlišný od ostatních útoků a je použitelný jen na některá zařízení stejně jako Bluesnarfing, například Sony Ericsson T610, Nokia 6310i,

Motorola V600, a další zařízení. Zranitelnost spočívá v tom, že některá zařízení dovolí uživateli vytvořit sériové spojení, které dovolí plný přístup ke kontrolnímu souboru cílového zařízení. Pro vážnost z Bluebug útoku nebyly uveřejněny žádné detailnější informace o způsobu provedení útoku. Novější zařízení jsou proti Bluebug chráněna důkladnější kontrolou přetečení zásobníku.

Automobilový šeptač (Car Whisperer)

Automobilový šeptač je útok, ke kterému se používá software, který dovolí útočníku poslat a přijmout zvuk z Bluetooth zvukové výbavy auta. Opět platí vzdálenost okolo 10m, bez specielního zařízení.

Červ Kabina

Červ Kabina je záludný software, je také známý jako malware. Této červ využívá ke svému šíření mobilní telefony a posílá se přes Bluetooth technologii. Tento červ je problémem zatím jen operačních systému Symbian series60 s Bluetooth. Výrobce Symbian již podnikl příslušné kroky k vyřešení tohoto problému.

Odstřelovač (BlueSniper Rifle)

John Hering se svým týmem Flexilis vytvořil tzv. Bluetooth pušku. Dostřel má o trochu větší než jeden kilometr, což znamená, že dokáže detekovat Bluetooth zařízení na vzdálenost okolo 1km. BlueSniper byla zkoušena na v Los Angeles na budovu US Bank, hned za pár minut se podařilo detekovat asi 20 aktivních zařízení s jejich MAC adresami. S tímto zařízením lze jak přijímat, tak vysílat. Otvírá se tím velká debata ohledně šíření virů jako je Kabina a další. Při použití vícero zařízení jako je BlueSniper by šlo sledovat pohyb zařízení a tím i pohyb majitele.

Podle Johna Herinka je výroba velmi snadná a finančně v celku nenáročná, až na srdce celého zařízení - 400MHz Gumstix 400f-bt v hodnotě necelých dvou set amerických dolarů, se pohybuje řádově v desítkách dolarech.

Skupina Flexilis měla za cíl, pouze upozornit na hrozící nebezpečí, nikoli toho zneužívat, proto kontaktovala SIG. Reakce SIG byla v celku doporučující ohledně opatrnosti, aktualizace softwaru a antivirového programu.

Jak říká John Hering: "*Naším cílem je, aby si veřejnost více uvědomovala problémy s bezpečností u bezdrátových technologii. Bluetooth je široce rozšířeno a mnoho lidí nemá ani tušení, co všechno lze provést s jejich zařízením na dálku !* " [12]

Obrázek 5.2 – John Hering a jeho Bluetooth puška

5.2. Obrana proti útokům

Výrobci mobilních a jiných zařízení vyvíjejí aktualizace proti těmto útokům, které jsou dostupné na jejich stránkách.

Bluetooth SIG nemůže garantovat stoprocentní bezpečnost. Bezpečnost je stále pokračující úsilí a snaha o řešení vznikajících problémů. Pro Bluetooth SIG má bezpečnost již od prvních okamžiků vysokou prioritu. Od prvního dne až do dnes se tato snaha ukazuje jako velmi dobrý krok. Práce v této oblasti stále pokračují v před a snahou je, aby se bezpečnost držela minimálně o krok před lidmi, kteří se snaží zneužívat těchto mezer.

[4] [10]

5.3. Nebezpečnost Bluetooth

Pohledem z druhé strany kritiků Bluetooth bezpečnosti. Jeden z velkých ohlasů je od velmi známé a zkušené firmy na bezpečnost Symantec, podle jejich slov by mohla SIG udělat mnohem víc kroků k bezpečnější komunikaci mezi Bluetooth zařízeními. Vychází z nových hrozeb, nebezpečí ve formě červů. Jedním z nejméně bezpečných Bluetooth zařízení jsou právě mobilní telefony a tzv. chytré telefony (Symbian). Podle některých zdrojů v tomto případě SIG dala přednost masovému rozšíření a jednoduchosti naproti větší bezpečnosti. Odborníci se shodují na tom že, Bluetooth má nejvíce slabé stránky v délce šifrovacího klíče, stejně jako v nebezpečném posílání hlavního klíče.

Zneužití Bluetooth v dnešní době není žádným problémem, může to provést každý, kdo by jen trochu chtěl. Na internetu jsou kompletní návody. Dnes už nepomůže ani často zmiňovaná vzdálenost 10m, díky BlueSniper je možné i na velkou vzdálenost zaútočit. Takřka by se dalo říci: "*Bezpečné Bluetooth, vypnuté Bluetooth.*" Bluetooth má opravdu široké použití, ale není vhodné ho používat v případech kde jde opravdu o bezpečí dat.

5.4. Základní bezpečnostní rady

Je tedy možné používat Bluetooth bezpečně? Bezpečnostním průnikům se lze vyhnout, pokud dodržujeme určitou opatrnost. Základní bezpečnostní doporučení jsou shrnuty v následujících bodech:

- Vždy při spárování dvou zařízení používejte heslo či klíč.
- Nepárujte se se zařízením, které neznáte. Dáváte mu úplný přístup k vašemu zařízení.
- Vypínejte funkci Bluetooth, když ji nepotřebujete.
- Pokud Bluetooth potřebujete zapnout, zkontrolujte, zda zařízení je v módu "hidden" či "invisible".
- Aktivujte další bezpečnostní vrstvy vašeho zařízení (pokud jsou dostupné).
- Pokud je Bluetooth zařízení ukradeno, vyškrtněte ho ze seznamu důvěryhodných zařízení (se kterými se vaše zařízení párovalo).
- Pokud vaše zařízení má antivirový software, pravidelně ho aktualizujte.
- Kontrolujte jednou za čas aktualizace ovladačů od výrobce

[11]

6. Příklady použití Bluetooth v praxi

Prvotní zamýšlená aplikace Bluetooth/802.15.1 byla pro domácí sítě: komunikace mezi mobilními komunikačními zařízeními (PDA, telefon apod.) a periferními zařízeními (zejména tiskárnami) nebo počítači pro sdílení a přenos souborů, tisk, elektronickou komunikaci. Kromě komunikačních a výpočetních systémů lze Bluetooth využít i pro komunikaci se spotřební elektronikou a domácími spotřebiči.

Bluetooth má však ještě další želízko v ohni, pokud jde o jeho budoucí uplatnění. Stává se totiž podstatnou součástí telekomunikačních systémů v automobilech, které začínají sloužit na cestách nejen jako prostředky navigace, asistence a přístupu k potřebným informačním zdrojům (včetně přístupu k Internetu), ale i jako vnitro-automobilová komunikace mezi osobními elektronickými zařízeními a elektronickým vybavením automobilu.

Kdo by kdysi čekal, že pračka bude schopna pomocí Bluetooth si sama stahovat přes domácí terminál z internetu prací programy pro různé druhy prádla nebo nahlásit domácímu terminálu poruchu, pokud nastane. Takovouto pračku vyrábí firma Toshiba.

6.1. Nejstarší použití Bluetooth v BT PC kartách

Jedno z nejčastějších použití bluetooth technologie je pomocí Pc-katry pro PC. Tyto karty vám umožní přidání Bluetooth do vašeho domácího počítače pouhým vložením PCMCIA karty do slotu na základní desce počítače. Jedna z prvních byla společnost IBM, která začala nabízet bezdrátové Bluetooth karty pro své notebooky ThinkPad. V dnešní době se Bluetooth dostalo na miniaturní velikosti, takže není překvapením, že je k dostání Bluetooth SD karta.

Obrázek 6.1 – PCMCIA Bluetooth karta

Obrázek 6.2 – Bluetooth SD karta od Toshiby

6.2. Srolovatelná textilní Bluetooth klávesnice - Bluetooth Fabric Keyboard

Společnost Eleksen vyvinula technologie, které umožňují zašít senzory, spoje a obvody do textilie - a lze je tak i vyrábět. Mimo doteků mohou tyto speciální chytré látky měřit i vlhkost. Na pravé straně textilie je umístěna malá krabička, ve které se skrývá vysílač s modulem Bluetooth a místo pro dvě baterie AA. Díky úspornému přístupu a nízkému příkonu i během plného provozu má jedno nabití vydržet 10 hodin. Látková část Bluetooth Fabric Keyboard je srolovatelná a tak může být snadno transportována. [5]

Obrázek 6.3 – Srolovatelná textilní Bluetooth klávesnice

6.3. Bezdrátové Bluetooth reproduktory Saitek 2.1

Saitek Wireless 2.1 Speaker System A-250, tak zní celý název zajímavé periferie, která by mohla nadchnout nejen příznivce všeho mobilně nezávislého. Tyto reproduktory nepotřebují žádné kabely k připojení k notebooku či PC - a současně si vystačí bez napájecího kabelu a zdroje.

Přes rozhraní Bluetooth je přenášen zvuk na vzdálenost až 30 metrů, při nižší kvalitě zvuku až 100 metrů. Pomocí vícero ovládacích prvků (hlasitost, Play, Pause, Stop, vpřed a zpět) a LCD displeje lze navíc ovládat přehrávání na PC či notebooku vzdáleně přímo z reproduktoru - a podle potřeby přerušit přehrávání či přeskočit několik skladeb.

Pro napájení jsou potřeba podle potřeby čtyři tužkové baterie typu AA (či akumulátory stejné velikosti), s nimiž má být možné dosáhnout až 20 hodin provozu. [6]

Obrázek 6.4 – Bezdrátové Bluetooth reproduktory

6.4. Bluetoothová myš MoGo

Mouse BT má netradiční design s rozměry vizitky. Díky tomu jí můžete mít, pokud jí zrovna nepoužíváte, uloženou ve slotu pro PC Card, přes který se MoGo také dobíjí. Plně nabitá je myš za méně než hodinu. [7]

Obrázek 6.5 – Bluetooth myš velikosti vizitky

6.5. Bezdrátová sluchátka

Bezdrátová stereo sluchátka s označením BT-120 HP jsou základním kamenem celé řady bezdrátových produktů firmy Ovislink. Jejich vzhled je sice nepředurčuje k lovu obdivných pohledů, ale co se funkčnosti týče, jsou na tom velmi dobře. Stříbrné středy obsahují hlavní ovládací prvky – na pravém se umístilo tlačítko pro zapnutí headsetu, na levém multifunkční joystick určený k ovládání hlasitosti, příjmu hovoru, či dokonce k ovládání hudebních funkcí proslaveného iPodu. Na levém sluchátku se navíc umístil i malý zobáček, v němž je umístěn mikrofon.

Kvalita podávaného zvuku je jen průměrná, při vyšších hlasitostech se zcela ztrácí hloubky. Frekvenční pásmo audio signálu je standardně 22 Hz až 22 kHz. Vestavěná baterie dokáže sluchátka napájet přibližně šest a půl hodiny.

Obrázek 6.6 – Bezdrátová sluchátka Ovislink

Sluchátka se dají obohatit o jednu ze čtyř různých přídavných zařízení, jejichž kombinací můžete ze sluchátek udělat doplněk k vaší hifi soustavě či jinému zvukovému zdroji s audio výstupem či stereo headset k počítači. Samotná sluchátka můžete použít jen pro použití s mobilním telefonem.

Zcela opačnou funkci pak zajišťuje Bluetooth Audio Receiver (přijímač), který z výše zmiňovaného vysílače dokáže signál přijmout a poslat ho do jakýchkoli vámi zvolených sluchátek

Obrázek 6.7 – Bezdrátový vysílač zvuku

Obrázek 6.8 – Bezdrátový přijímač zvuku

Dalším z řady produktů je USB dongle. Ten vám zajistí velmi pohodlný poslech hudby v okolí vašeho počítače, díky zabudovanému mikrofonu ve sluchátkách lze použít toto spojení i jako velmi příjemný headset pro internetovou komunikaci.

Posledním zajímavým zástupcem od firmy Ovislink je modul určený speciálně pro použití s legendárním iPodem. Modul umožňuje i bezdrátově iPod ovládat. [8]

Obrázek 6.9 – USB přijímač a vysílač - USB dongle

Obrázek 6.10 – Bezdrátový ovládač iPodu

6.6. Zpětné zrcátko s Bluetooth

Vlastně jde o šikovné handsfree. Zpětné zrcátko se přes Bluetooth 1.1 spojí s mobilním telefonem nebo komunikátorem a zobrazuje číslo příchozího hovoru... Zobrazené číslo může mít až 12 cifer. Na spodní hraně zrcátka jsou tlačítka pro příjem a ukončení(odmítnutí) hovoru, ale také tlačítka na regulaci hlasitosti vestavěného reproduktoru pro hlasitý poslech.

Obrázek 6.11 – Zpětné zrcátko s Bluetooth

6.7. Šíře použití a možnosti budoucnosti

Použití je celá řada, pro přehled jsou uvedeny kategorie a nejčastější použití

- Počítače, notebooky, PDA, tiskárny, digitální fotoaparáty, kamery, přístupové sítě, modemy
- příslušenství – klávesnice, myši, joysticky, bezdrátová sluchátka, speciální digitální tužka, která přenáší psaný text do SMS v mobilním telefonu nebo jiného zařízení
- Mobilní telefony, bezdrátové headset sady
- MP3 přehrávače, ledničky, pračky, navigační zařízení GPS, automobily, hodinky
- Karty Compact flash, SD karty, USB moduly, PSMCA katry
- Otevírání dveří, dálkový přístup, ovládání přístrojů

Obrázek 6.12 – Bluetooth digitální tužka

Obrázek 6.13 – Bluetooth PDA klávesnice

V budoucnu aplikační možnosti závisí víceméně na fantazii vývojářů a integrátorů, mohou to být:

- posílání digitálních fotografií z Bluetooth fotoaparátu přes mobilní telefon
- identifikační systémy (založené na malém dosahu Bluetooth)
- platební systémy spojené s identifikací (garážová stání)
- automatické nastavení / vypnutí zvonění (v kostele, na koncertu...)
- skryté události přenosu informací (mobilní telefon po přijetí faxu/mailu probudí notebook ze sleep modu, provede přenos a zase ho uspí)

7. Hardwarové řešení, výběr komponent

Pří výběru zařízení mikrokontroleru nebo Bluetooth jednotky jsou důležité faktory jako cena, výkon, spotřeba a napájení, pouzdro, počet pinů, velikost paměti, způsob programování, periférie. Pro naši potřebu byly nejvíce určujícími parametry cena, dostupnost a základní parametry. Nejtěžší bylo obstarat Bluetooth čip, na českém trhu jsou těžko k sehnání. Zpravidla je třeba nechat si ho poslat ze zahraničí. Nakonec se podařilo zajistit Bluetooth modul německé firmy Amber-Wireless BlueNiceCom III. Výhodou tohoto modulu je velmi dobrá základní výbava, integrovaná anténa a obsažený profil pro sériovou komunikaci v modulu.

Výběr řídícího mikrokontroleru byl oproti problematickému nalezení bluetooth modulu velmi lehký, na trhu je nesrovnatelně větší množství možností. Pro naše účely postačí jednoduchý, levný a dostupný mikrokontroler od firmy Atmel Atmega8. Dalšími kritérii pro výběr byl počet použitelných programovatelných pinů a snadné programování, což díky softwaru AVRstudiu Atmel také splňuje. V případě potřeby lze zvolit i modul s větší pamětí Atmegu16.

7.1. Řídící mikrokontroler

Programovatelný mikrokontroler je dodáván i s příslušným softwarem AVR Studio, usnadňující programování a navázání spojení s čipem. Atmega8 je 8bitový CMOS mikroprocesor s nízkou spotřebou energie postavený na architektuře AVR RISC. Atmega8 dosahuje výkonností blížící se 1 MIPS za MHz, což dovoluje systémovému návrháři optimalizovat příkon versus rychlost zpracovávání. Atmega8 také disponuje 6 nebo 8 kanálovým 10bitový A/D převodníkem. Lze využít 23 programovatelných vstupů a výstupů. Atmega8 využívá 32 registrů spojených přímo s výkonnou jednotkou ALU. [14]

Technické parametry Atmegy8 jsou tyto:

Obrázek 7.1 – Pouzdro modulu Amega8

Flash – programovatelná paměť	**8 Kb**
EEPROM	**0,5 Kb**
SRAM – static ram	**1024 b**
Max I/O Pins – počet vstupů a výstupů	**23 pins**
F.max – maximální frekvence	**16 MHz**
Vcc – napájecí proud	**2,7 – 5,5 V**

tabulka 7.1 – Technické parametry Atmega8

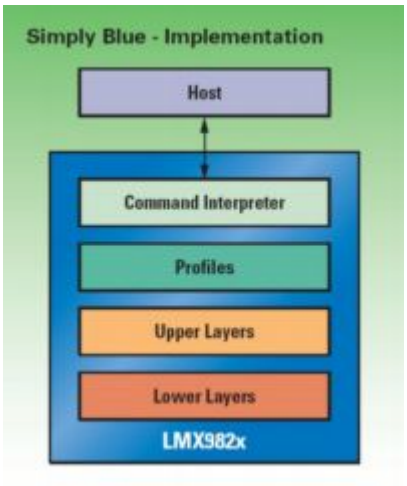
7.2. Bluetooth modul

Základní charakteristické prvky modulu BlueNiceCom III

- Bluetooth druhé třídy
- Může být v síti master i slave
- Implementován profil sériové komunikace – SPP (Serial Port Profile)
- UART rozhraní (sériová linka)
- Integrovaná čipová anténa
- Podpora GAP & SDP – popsané již v kapitole 2.3.1 Základní profily

Bluetooth modul BlueNiceCom III s integrovanou anténou od německé firmy Amber-Wireless je postavený na základu LMX9820A od National Semiconductor. Je to levný modul s kompaktní komunikační výbavou, určený pro sériový přenos dat. BlueNiceCom má integrovaný SPP profil pro sériovou komunikaci, se kterým může komunikovat s ostatními Bluetooth zařízeními, které podporují stejný profil. K procesoru je modul připojen pomocí UART rozhraní. Všechny ostatní profily mohou být nahrány díky SPP profilu přes PC nebo externí procesor, například: profil vytáčeného připojení , Fax profil, profil pro síť LAN. Modul má integrovanou anténu v čipu, ale je možné přidat

externí anténu. Řízení a nastavování čipu obsluhuje externí procesor. Jednotka může pracovat v pico síti jako Master - nadřazený uzel až pro 3 Slave - podřazený zařízení nebo jako Slave, to záleží na nastavení a použité aplikaci. Při komunikaci bod – několik bodů (point-to-multipoint, což je síť piconet) je nezbytné řízení pomocí mikroprocesoru. [15]



Obrázek 7.2 – Vrstvy obsažené v modulu LMX982x

Technické parametry modulu a pouzdro

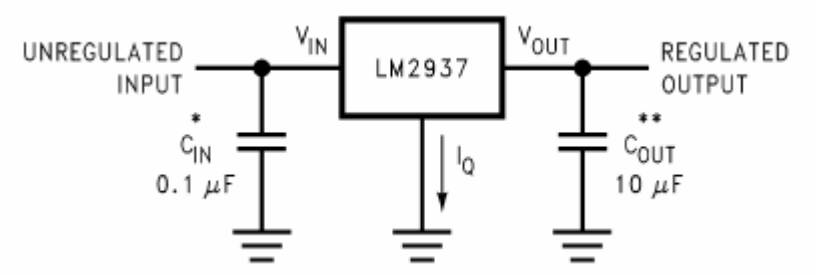
Obrázek 7.3 – Bluetooth přípravek BlueNiceCom III

Napájecí napětí	**2,85 do 3,6 VDC**
Odběr proudu Tx, Rx	**65mA**
Vysílací výkon	**2mW**
Výstupní citlivost	**- 77 dBm**
Přenosová rychlost UARTu	**9,6 kbps až 115 kbps**
Provozní teplota	**od -30°C do +85°C**
Anténa	**Integrovaná čipová anténa**
Rozměry	**27,5 x 16 x 3,5 mm**

tabulka 7.2 – Technické parametry BlueNiceCom III

7.3. Obvod napájecího napětí

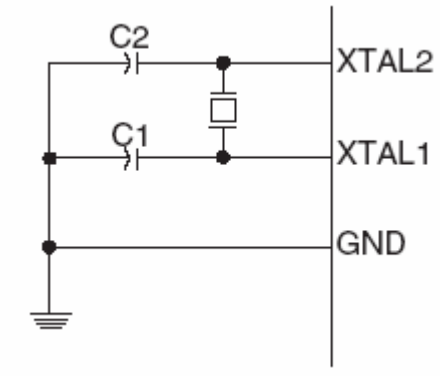
Jako stabilizátor napětí jsem použil jednoduchý obvod LM2937 - 3.3, který stabilizuje napětí ze vstupních 5V nebo vyššího napětí na našich požadovaných 3,3V s tolerancí 5% pro mikrokontroler i Bluetooth modul. Dodávaný výstupní proud je 400mA. LM2937 vyžaduje na výstupu kondenzátorovou propojku (bypass) se zemí pro dobrou stabilitu obvodu. Jako u většiny PNP regulátorů je ESR (ekvivalentní sériový odpor) kondenzátoru nejkritičtější konstrukční parametr, ale obvod LM2937 osahuje speciální náhradní schéma kompenzující toto nebezpečí. Obvod je stabilní pro teplotní rozsah od -40°C do +125°C a má vestavěnou tepelnou ochranu. [16]



Obrázek 7.4 – obvod stabilizátoru napětí

7.4. Řízení hodin mikrokontroler

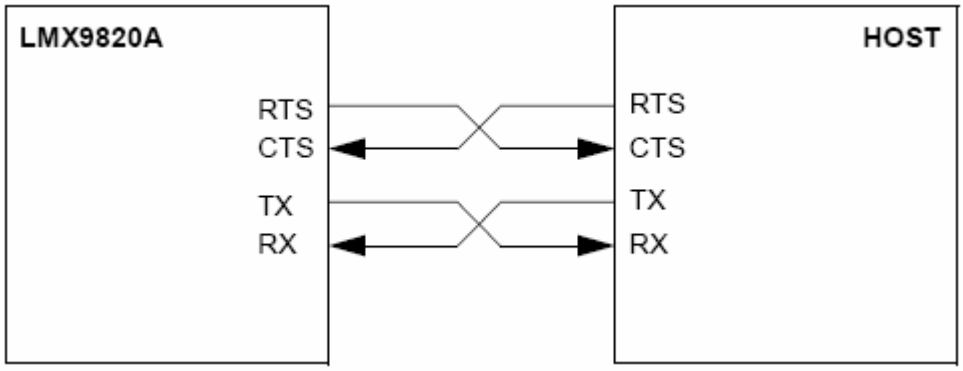
Pro řízení hodin v mikrokontroleru je možné použít RC rezonanční obvod, externí hodiny nebo krystalový oscilátor. Pro naše účely postačí jednoduchý krystalový oscilátor s frekvencí 8MHz, připojený na I/O piny XTAL1 a XTAL2. Velikost kapacit kondenzátorů byl zvolen 27pF. Podle doporučené hodnoty.



Obrázek 7.5 – Zapojení krystalu oscilátoru

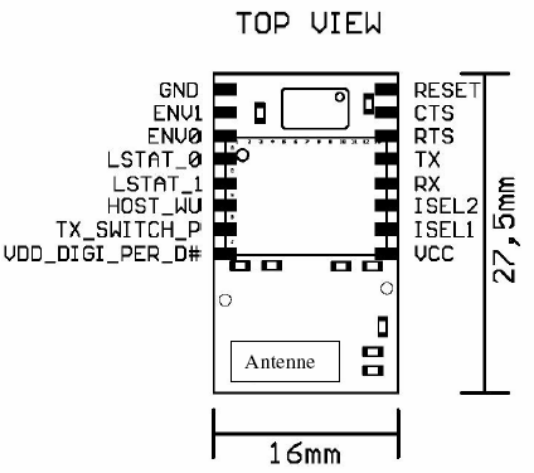
7.5. Připojení pinů BT modulu s řídícím mikrokontrolerem

Napájecí piny Bluetooth modulu a mikrokontroleru jsem připojil na stabilizované napájecí napětí 3,3V pomocí obvodu LM2937. Společně jsem je uzemnil přes GND piny na zem a mezi napájení a zemnění vložil vyhlazovací kondenzátor.

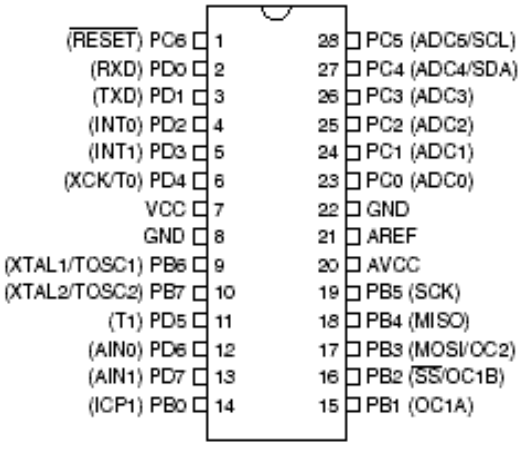


Obrázek 7.6 – propojení kanálu Rx Tx

Komunikační signály Rx a Tx jsem z řídícího mikrokontroleru Atmegy8 (Host) připojili křížem s BT modulem na piny Tx, Rx. Signalizační kanály přenosu RTS CTS jsem propojily s programovatelnými I/O vstupy Int0 a Int1. Ostatní piny Bluetooth modulu jsou připojeny na zbylé I/O vstupy Atmegy. Reset BT modulu je připojen též na I/O Atmegy a RESET Atmegy je připojen přes 10KΩ odpor na napájení.



Obrázek 7.7 – Piny u Bluetooth modulu



Obrázek 7.8 – Piny u Atmegy8

Schéma zapojení BT modulu a mikrokontroleru bylo vytvořeno v Eaglu (příloha A)

8. Průběh komunikace a možnosti programování

8.1. Komunikace mezi BT modulem a mikrokontrolerem

BT modul LMX9820A je obsluhován mikrokontrolerem přes rozhraní UART. Příkazy se posílají ve specielním formátu paketu.Je-li BT modul přepnut do Transparent Modu mikrokontroler přijímá pouze data bez formátovacího paketu.

Start delimiter	Packet Type identification	Op code	Data length	Check-sum	Packet Data	End delimiter
1 byte	1 byte	1 byte	2 bytes	1 byte	<Data length> bytes	1 byte
	|---------- Checksum ----------|					

Obrázek 8.1 – formát komunikačního balíku

Start delimiter – znak ukazující na začátek nového paketu. STX = 0x02

Packet Type identification – identifikace druhu paketu. K dispozici jsou 4 typy, dotaz, potvrzení, odpověď a informační. Opět jsou charakterizovány

Opcode – specifické příkazy charakterizované určitým bytem**.**

Data length – délka pole packet data. Maximum je 333 bytů.

Checksum – kontrolní součet délky dat, specifického příkazu a typu balíku. Názorná ukázka je vidět na obrázku 8.2

Packet data – pole dat je v binárním kódu.

End delimiter – znak ukončení ETX = 0x03

8.1.1. Příklad průběhu komunikace

Ukázka jednoduchého možného průběhu komunikace mezi BT modulem a mikrokonrolerem při navázání a přenosu dat mezi dvěmi BT zařízeními. Při programování lze zahrnout další služby a možnosti jako je volba bezpečnosti přenosu, komunikace při nedostatku energie, uspání a vzbuzení zařízení, změna komunikačních portů a další možnosti.

Přehled průběhu komunikace.:

- Hledání zařízení
- Vytvoření SDAP žádosti o spojení a nalezení služeb
- Vytvoření SPP spojení
- Transparentní mód pro přenos dat
- Zrušení spojení

Prvním krokem pro navázání spojení je objevení zařízení (Inquiry). Příslušný příkaz Opcode je GAP_INQUIRY a GAP_DEVICE_FOUND.

Následuje výměna fyzických adres BD_Addr a výkonnostních tříd zařízení. Po tomto kroku je nutno používat oddělené příkazy. Opcode - GAP_REMOTE_DEVICE_NAME

K ustanovení SDAP spojení je potřeba BD_addr, ale také RFComm číslo komunikačního portu, a zaregistrovaný profil, který bude použit pro komunikaci. SDAP má za úkol prozkoumat a najít všechny dostupné a nabízené služby spojovaného zařízení. Navázání spojení SDAP příkazem Opcode SDAP_CONNECT, průzkum a nalezení služeb SDAP_SERVICE_BROWSE, SDAP_SERVICE_SEARCH. Odpověď na dotazy dostane seznam služeb SDAP_SERVICE_REQUEST. Po dokončení se spojení SDAP odpojuje SDAP_DISCONNECT.

Po nalezení použitelných služeb následuje fáze navázání plného spojení pomocí SPP (serial port profile) SPP_ESTABLISH_LINK, k navázání spojení je potřeba BD_Addr a RFComm řídící port, který byl získán již při SDAP spojení. Jako odpověď se vrací potvrzení ustanovení spojení SPP_LINK_ESTABLISHED.

V tomto bodě může být spojení přepnuto do transparentního modu vhodnějšího pro přenos dat v rámci SPP spojení nebo můžeme přenášet data pomocí služby SPP příkazem v Opcode SPP_SEND_DATA a odpovědí na přijetí SPP_INCOMING_DATA.

Vhodnější je ustanovit pro přenos dat transparentní mód. Pro ustanovení modu je nutné aby bylo navázané spojení SPP. Základním rozdílem je, že mimo transparentní mód jsou data obalena komunikačním paketem, kdežto při transparentním módu jsou posílána pouze data. Ustanovení tohoto módu se provádí Opcodem SPP_TRANSPARENT_MODE

Po ukončení transparentního módu dochází k obnovení SPP spojení SPP_RELEASE_LINK s odpovědí SPP_LINK_RELEASED a případnému ukončení spojení.

8.2. AVR Studio a alternativy

Firma Atmel poskytuje na svých stránkách zdarma ke stažení programovací prostředí AVR Studio pod GNU licencí pro své mikroprocesory. V prostředí AVR lze programovat v jazyku C nebo asembleru. Výsledný program se kompiluje do zdrojového souboru typu HEX (hexadecialní soubor), který je srozumitelný mikroprocesorům AVR. Studio slouží zároveň i jako simulační program, zobrazuje obsahy registrů, monitoruje vstupy / výstupy a poskytuje mnoho dalších informací. V tomto studiu jsou již obsaženy příslušné knihovny a nastavení pro usnadnění navázání spojení, výběr rychlostí, výběru napájecího napětí a dalších parametrů.

Obrázek 8.2 – Vývojové prostředí od Atmelu AVR Studio

Firma Atmel podporuje podobné prostředí jako je AVR Studio, vše pod licencí GNU (freewarová licence). Tyto prostředí samozřejmě podporují především práci s mikrokontrolery AVR.

- CodeVisionAVR – vyznačuje se jednoduchostí a snadným ovládáním. Komfortní prostředí s minimem nastavování.
- ImageCraft – levná varianta programového prostředí pro mikroprocesory AVR, ImageCraft umožňuje kompresi kódu.
- IAR EW-AVR – prostředí podporující mnoho značek mikroprocesorů.

Hyperterminal

Hyperterminal je standardní součástí Windows 2000/XP. Pomocí jeho lze navázat spojení přímo s BT modulem nebo přes sériovou linku s Atmegou. Nejčastěji slouží k ověření funkčnosti komunikace a zkušebnímu přenosu dat.

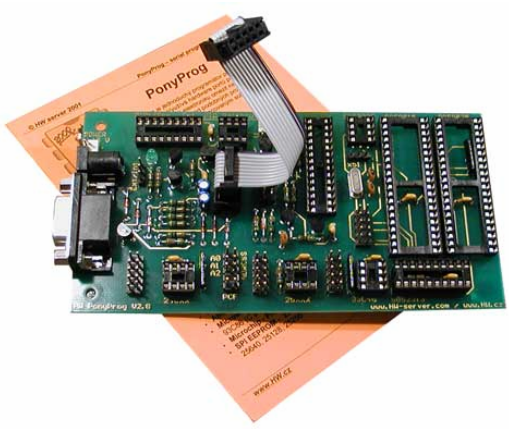
Simply Blue Commander

K BT modulu LMX9820A od National Semiconductor je s dokumentací dodávána jednoduchá softwarová aplikace Simply Blue Commander sloužící pro nastavení všech důležitých parametrů modulu (jméno modulu, PIN kód, rychlost UART spojení, pracovní režim, atd.).

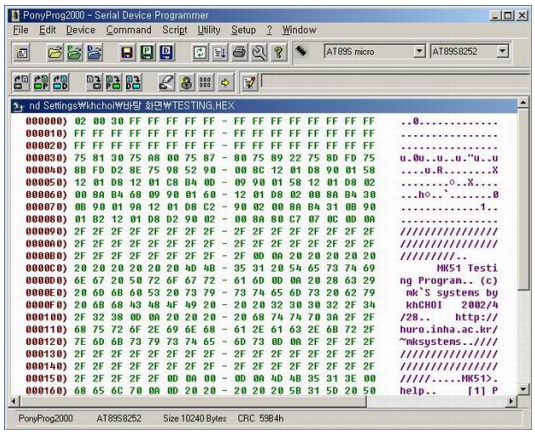
8.3. Software PonyProg 2000

Jako zajímavá možnost snadného spojení mikrokontroleru s počítačem a snadného programování je projekt PonyProg 2000. Projekt Claudia Lanconelliho má dvě části softwarovou a hardwarovou. Pro hardware je základem deska osazená několika druhy patic pro čipy. Podporovaných čipů je přes 90 typů od výrobců I²C Bus, Microwire, Atmel AVR nebo Microchip a dalších. Deska si rozumí s dodávaným softwarem ve všech běžných operačních systémech od Win95 - XP a je připravena podpora i pro Intel Linux. Softwarová aplikace je velmi jednoduchá na ovládání, stačí vybrat příslušný komunikační port, správný mikroprocesor a použít tlačítka pro nahrávání a mazání programu v samotném čipu.

Deska pro PonyProg je snadno dostupná na www.hw.cz a příslušný software je zdarma ke stažení na stránkách www.lancos.com .[17]



Obrázek 8.3 – Hardware pro PonyProg



Obrázek 8.4 – Software pro PonyProg

Závěr

Touto prací se podařilo zmapovat historii a průběh vývoje bezdrátové technologie Bluetooth. Popsány jsou principy fungování, technické specifikace této technologie, způsoby navazování spojení a seskupování do sítí. Poukazuje na bezpečnostní rizika a shrnuje základní pravidla pro bezpečné párování. V tomto směru má Bluetooth jisté mezery, které by mohly do budoucna znepříjemnit další rozšíření a popularitu technologie. Nastiňuje šíři využití technologie v domácnostech, provozech a práci. Díky své ceně a schopnostem se budeme častěji setkávat se zařízeními tohoto typu, prakticky denně při maličkostech. Budoucí použití závisí převážně na fantazii vývojářů a integrátorů. Práce konkrétním příkladem ukazuje realizaci vytvoření funkčního Bluetooth modulu a mapuje možnosti programování.

Práci se nepodařilo dokončit v plném rozsahu zadání. Největší podíl na této skutečnosti měl problém nalezení a získání vhodného Bluetooth zařízení, což se sice podařilo, ale již v pokročilém čase. Zařízení bylo využito k praktické demonstraci propojení Bluetooth modulu BlueNiceCom III a řídícího mikrokontroleru Atmega8.

Práce si klade za cíl detailního popisu funkcí a schopností Bluetooth zařízení, příkladu praktického návrhu a zmapování možností programování. Podává kompletní a ucelený pohled na bezdrátovou technologii Bluetooth, ukazuje na její široké možnosti, propracovanou strukturu a velmi perspektivní budoucnost.

Použitím této práce je možno snadno a rychle získat přehled o principech fungování Bluetooth. Pokračovatelům usnadní výběr a realizaci hardwaru a nastíní softwarové možnosti a strukturu programu.

Seznam použitých zdrojů

[1] Pužmanová, Rita ; *Osobní sítě -- Bluetooth a IEEE 802.15* [online] 14-5-2002

http://www.lupa.cz/clanky/osobni-site-bluetooth-a-ieee-802-15/?SID=A9D79D6C19344424A01A744ED27F532A

[2] Hájek, Jan ; *Standard Bluetooth: vývoj, princip a možnosti využití* [online] ročník 48 • číslo 4 • duben 2005

http://www.automatizace.cz/article.php?a=639

[3] Řehák, Jan; *Osobní sítě - Bluetooth a IEEE 802.15* [online]

http://www.hw.cz/Rozhrani/Ethernet/ART917-Osobni-site---Bluetooth-a-IEEE-802.15.html

[4] Bluetooth Speciál Interest Grup ; *How Bluetooth works – Jak pracuje Bluetooth* [online]

http://bluetooth.com/

[5] Hyánek, Bohumil ; *TechNet - Klávesnice do ruličky a bezdrátově: Srolovatelná textilní Bluetooth klávesnice* [online] 13-1-2006

http://notebooky.idnes.cz/novinky/bttextilekeyboardpreview.html

[6] Hyánek, Bohumil ; *TechNet - Poslouchejte kvalitní zvuk přes Bluetooth a na baterie* [online] 18-11-2005

http://notebooky.idnes.cz/novinky/saitekbluetoothmobilereproprv.html

[7] Škopek, Pavel *; TechNet - Chcete myš o rozměrech vizitky?* [online] 6-4-2004

http://technet.idnes.cz/hardware.asp?r=hardware&c=A060103_111822_hardware_psp

[8] Vysušil, Petr ; *TechNet – Testujeme bezdrátová sluchátka, která vám dají volnost* [online] 6-4-2004

http://technet.idnes.cz/tec_audio.asp?r=tec_audio&c=A051201_181242_hardware_hro

[9] Kačenka, Petr *; PalmServer - Zpětné zrcátko s Bluetooth* [online] 21-11-2005

http://www.palmserver.cz/clanek.php3?show=3294

[10] Spence, Michael se skupinou lidí ; *Security of Wireless Technologies* [online] http://www.cs.bham.ac.uk/~mdr/teaching/modules04/security/students/SS1A-wireless.pdf

[11] Eileen Yu, ZDNet Asia ; *Is Bluetooth still secure?* [online] 22-03-2006 http://www.zdnetindia.com/insight/security/stories/135604.html

[12] Cheung, Humphrey *; How To: Building a BlueSniper Rifle* [online] 8-03-2005 http://www.tomsnetworking.com/2005/03/08/how_to_bluesniper_pt1/

[13] Penn, Ivo ; *Bezdrátová Bluetooth technologie* [online] 2003 http://www.fei.vsb.cz/wofex/2003/paper/p2612/penn_ivo.pdf

[14] ATMEL ; *8-bit with 8K Bytes In-Systém Programmable Flash* [online] říjen 2004 http://atmel.com/dyn/resources/prod_documents/2486S.pdf

[15] AMBER WIRELESS ; *BlueNiceCom III V1.5* [online] duben 2005 http://www.promelec.ru/for_news/bluetooth/HE_BlueNiceCom_III_V1.5.pdf

[16] National Semiconductor ; *LM2937-2.5, LM2937-3.3 400mA and 500mA Voltage Regulators* [online] srpen 2005 http://www.national.com/ds/LM/LM2937-2.5.pdf

[17] LanCos ; *PonyProg* [online] poslední aktualizace Únor 2006 http://www.lancos.com/prog.html

[18] Arca/Wavecatcher ; *Bluetooth protocol analzyer* [online] 01-11-2001 http://www.arca-technologies.com/manuals/arcawavecatcher.pdf

Příloha A – Schéma zapojení BT modulu a mikrokontroleru Atmega8